ESET REMOTE ADMINISTRATOR 6

Installationsanleitung und Benutzerhandbuch

Klicken Sie hier, um die neueste Version dieses Dokuments zu öffnen.



ESET REMOTE ADMINISTRATOR 6

Support: www.eset.com/support

Versionsstand 20/05/2015

Inhalt

Inhalt

1. Einführung

ESET Remote Administrator (ERA) ist eine Anwendung, mit der Sie ESET-Produkte auf Arbeitsstationen, Servern und Mobilgeräten in einer Netzwerkumgebung von einem zentralen Standort aus verwalten können. Mit dem integrierten Taskverwaltungssystem von ESET Remote Administrator können Sie ESET-Sicherheitslösungen auf Remotecomputern installieren und schnell auf neue Probleme und Bedrohungen reagieren.

ESET Remote Administrator selbst bietet keinen Schutz vor Schadcode. Der Schutz Ihrer Umgebung hängt vom Vorhandensein einer ESET-Sicherheitslösung auf den Arbeitsstationen, Servern und Mobilgeräten ab, beispielsweise ESET Endpoint Security oder ESET File Security für Microsoft Windows Server.

ESET Remote Administrator 6 basiert auf zwei grundlegenden Konzepten:

1. **Zentrale Verwaltung** – Das gesamte Netzwerk kann von einem zentralen Punkt aus konfiguriert, verwaltet und überwacht werden.
2. **Skalierbarkeit** – Das System eignet sich gleichermaßen zur Bereitstellung in kleinen Netzwerk und in großen Unternehmensumgebungen. Durch Erweiterung/Skalierung kann das System schnell und einfach an die Entwicklung Ihrer Infrastruktur angepasst werden.

Auf den ESET Remote Administrator-Hilfeseiten finden Sie ein vollständiges Benutzeradministrationshandbuch. Machen Sie sich zunächst mit den grundlegenden Konzepten und Funktionen von ESET Remote Administrator vertraut:

- ESET Remote Administrator-Architektur
- Installationsprozeduren und Bereitstellungsprozeduren
- Agenten-Bereitstellung mithilfe von GPO und SCCM
- Erste Schritte nach der Installation von ESET Remote Administrator
- Erste Schritte mit der ERA-Web-Konsole
- Die Arbeit mit ESET Remote Administrator
- Administration
- Migrations-Tool

1.1 Funktionen

Die folgenden Funktionen und Eigenschaften sind neu in Version 6:

- Plattformunabhängigkeit – Der ERA-Server funktioniert unter Windows und Linux.
- Die ERA Web-Konsole ist die primäre Benutzeroberfläche für ESET Remote Administrator. Der Zugriff erfolgt über einen Webbrowser. So können Sie die Lösung von beliebigen Standorten und Geräten aus verwenden.
- Das komplett anpassbare Dashboard bietet einen guten Überblick über den Sicherheitsstatus des Netzwerks. Der Admin-Bereich der ESET Remote Administrator-Web-Konsole (ERA Web-Konsole) ist ein leistungsfähiges und benutzerfreundliches Tool für die Verwaltung von ESET-Produkten.
- Benachrichtigungen liefern in Echtzeit alle wichtigen Informationen. In Berichten können Sie verschiedene Datentypen bequem sortieren und zur späteren Analyse vorbereiten.

1.2 Architektur

Für eine vollständige Bereitstellung der ESET-Sicherheitslösungen müssen folgende Komponenten installiert werden (Windows-Plattform):

- ERA-Server
- ERA-Datenbank
- ERA-Web-Konsole
- ERA-Agent

Für eine vollständige Bereitstellung der ESET-Sicherheitslösungen müssen folgende Komponenten installiert werden (Linux-Plattform):

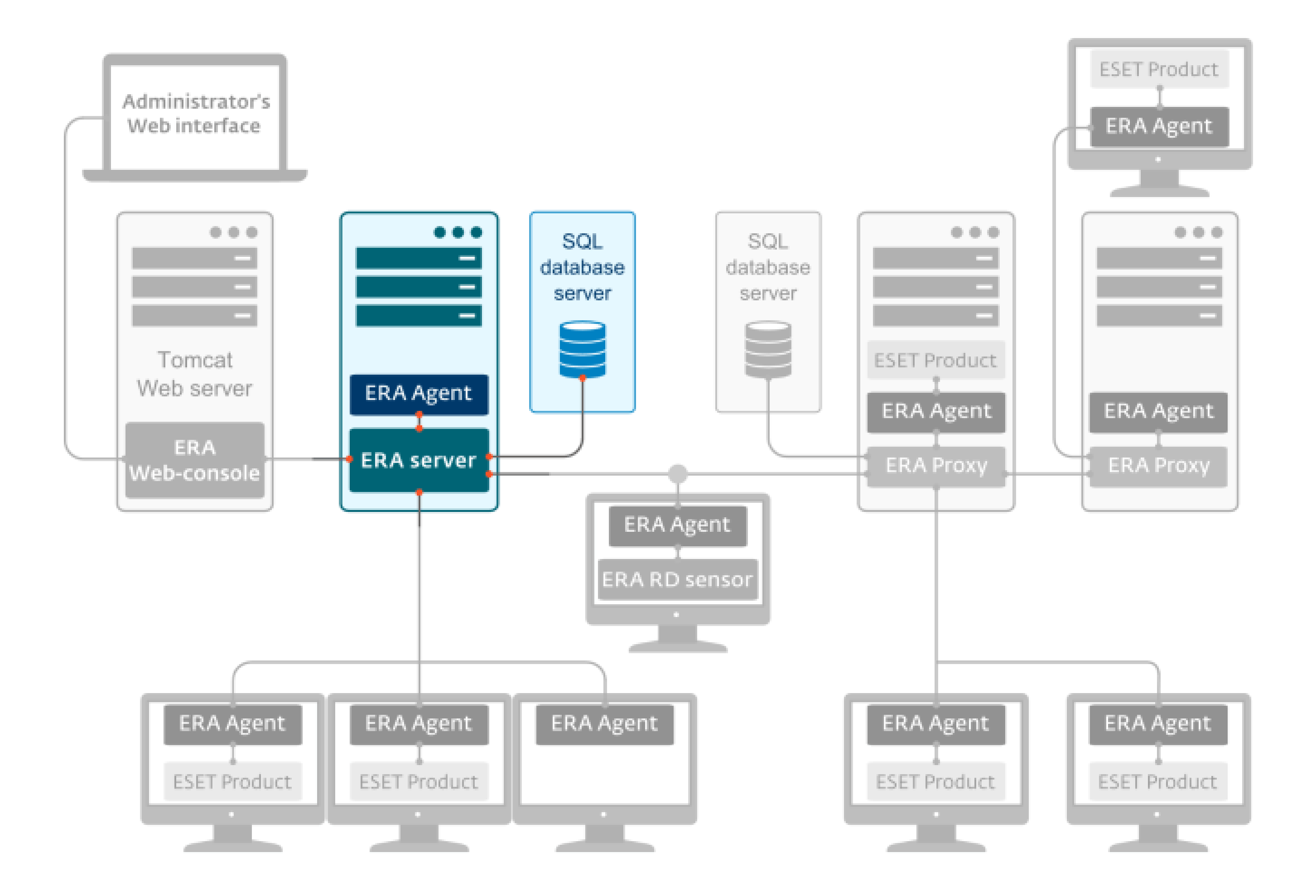
- ERA-Server
- ERA-Web-Konsole
- ERA-Agent

Die nachstehend aufgeführten unterstützen Komponenten sind optional. Wir empfehlen ihre Installation, um die Leistungsfähigkeit der Anwendung in Ihrem Netzwerk zu steigern:

- ERA-Proxy
- RD Sensor
- Connector für Mobilgeräte
- Apache-HTTP-Proxy

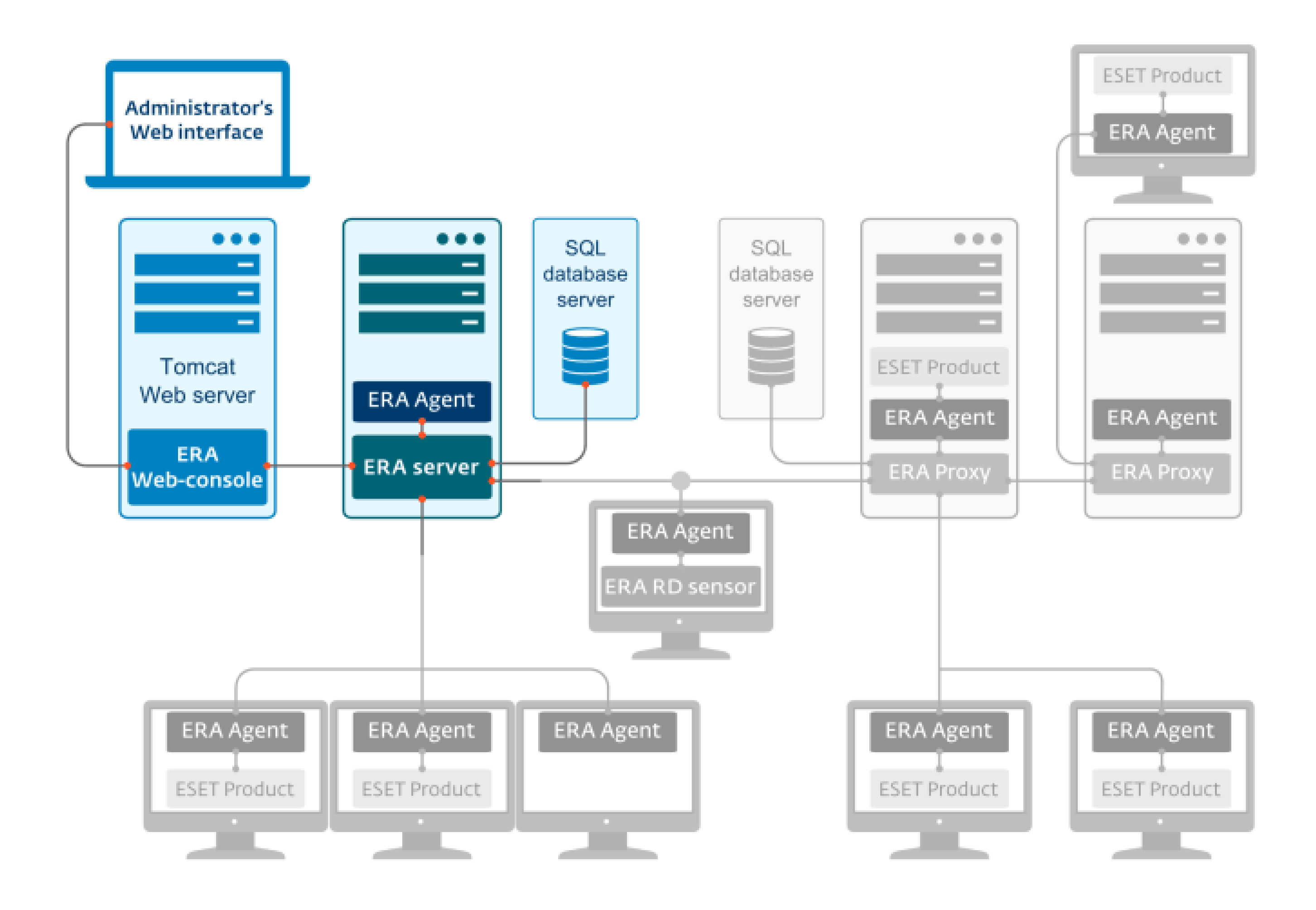
1.2.1 Server

ESET Remote Administrator Server verarbeitet alle Daten von den Clients, die über den ESET-Agenten mit dem Server kommunizieren. Für die ordnungsgemäße Datenverarbeitung benötigt der Server eine stabile Verbindung zu dem Datenbankserver, auf dem sich die Netzwerkdaten befinden. Wir empfehlen, den Datenbankserver auf einem anderen Computer zu installieren, um eine höhere Leistung zu erreichen.



1.2.2 Web-Konsole

Die ERA-Web-Konsole ist eine webbasierte Benutzeroberfläche, mit der Sie die ESET-Sicherheitslösungen in Ihrer Umgebung verwalten können. Sie bietet eine Übersicht über den Status der Clients im Netzwerk und kann zur Remote-Bereitstellung von ESET-Lösungen auf unverwalteten Computern verwendet werden. Der Zugriff auf die Web-Konsole erfolgt über einen Browser (siehe Unterstützte Webbrowser). Wenn Sie den Zugriff über das Internet auf den Webserver zulassen, können Sie ESET Remote Administrator von nahezu jedem beliebigen Standort und Gerät aus verwenden.



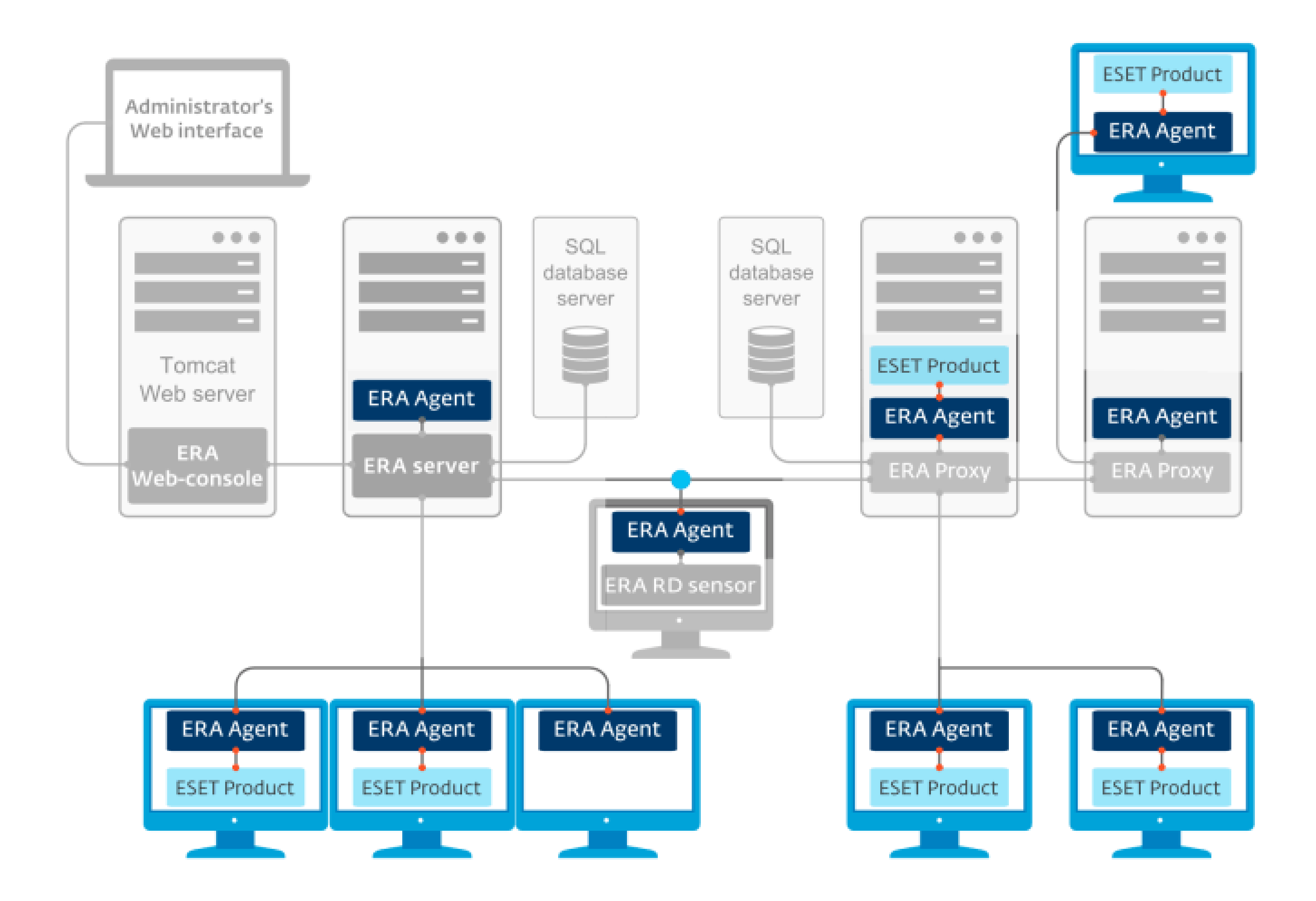
1.2.3 Agent

Der Agent ist ein wesentlicher Bestandteil von ESET Remote Administrator. Die Clients kommunizieren nicht direkt mit dem Server, sondern tun dies über den Agenten. Der Agent erfasst Informationen vom Client und sendet sie an den ERA-Server. Wenn der ERA-Server dem Client einen Task übermittelt, wird dieser Task an den Agenten gesendet, der ihn an den Client weitergibt.

Zur einfacheren Implementierung des Endpunktschutzes ist der autonome ERA-Agent in der ERA-Suite (Version 6 und höher) enthalten. Der Agent ist ein einfacher, hochmodularer und leichter Dienst, der die gesamte Kommunikation zwischen dem ERA-Server und beliebigen ESET-Produkten bzw. Betriebssystemen übernimmt. ESET-Produkte kommunizieren nicht direkt mit dem ERA-Server, sondern über den Agenten. Clientcomputer, auf denen der ESET-Agent installiert ist und die mit dem ERA-Server kommunizieren können, werden als „verwaltet" bezeichnet. Sie können den Agenten auf einem beliebigen Computer installieren, unabhängig davon, ob auf dem Computer eine ESET-Software installiert ist.

Vorteile des Agenten:

- Einfache Einrichtung: Der Agent kann als Bestandteil einer standardmäßigen Unternehmensinstallation bereitgestellt werden.
- Sicherheitsverwaltung vor Ort: Der Agent kann mit mehreren gespeicherten Sicherheitsszenarien konfiguriert werden, was die Reaktionszeit im Falle einer Bedrohung deutlich reduziert.
- Offline-Sicherheitsverwaltung: Der Agent kann auch ohne bestehende Verbindung zum ERA-Server auf ein Ereignis reagieren.



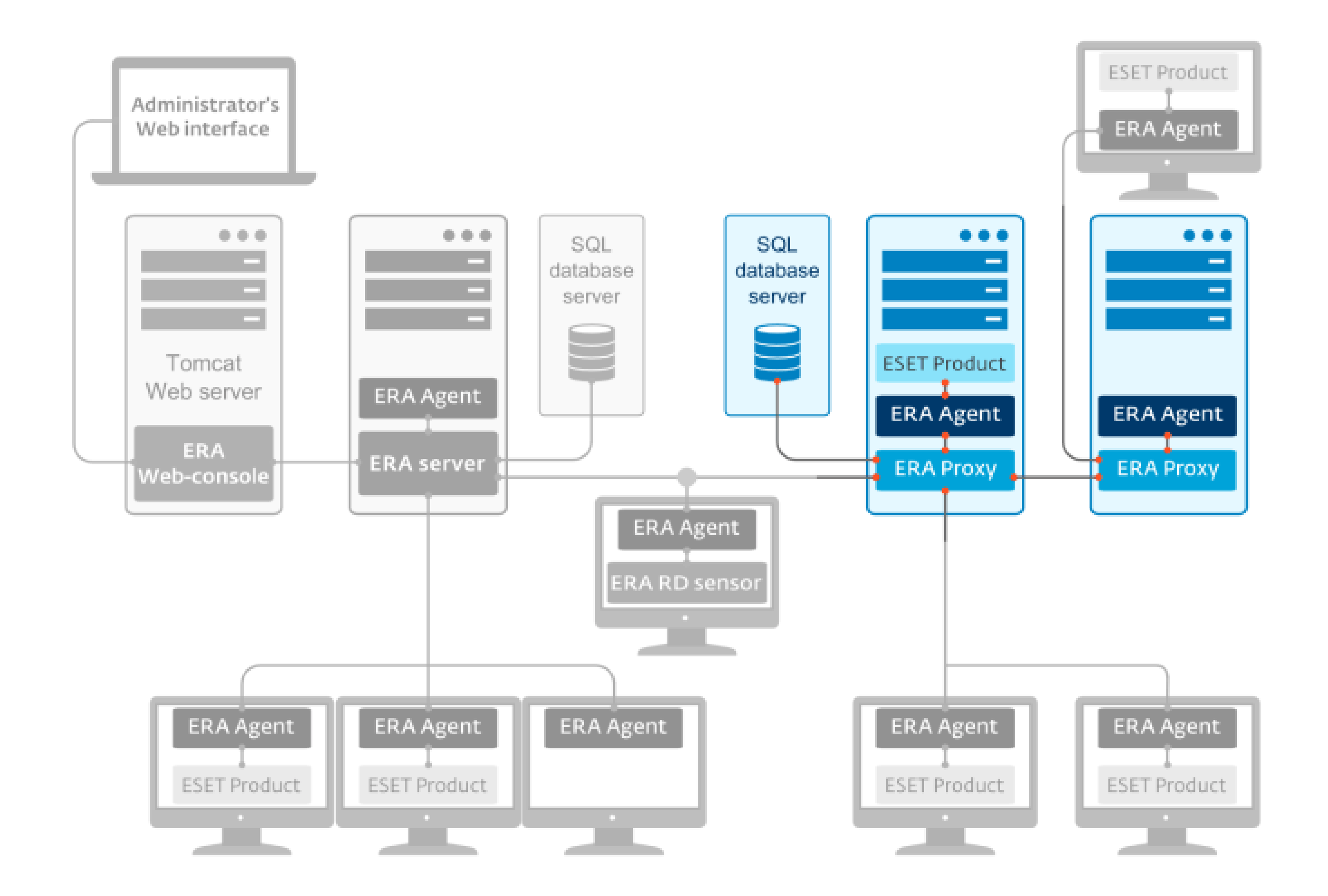
1.2.4 Proxy

Der ERA-Proxy ist eine leichtere Version der Serverkomponente. Diese Art Server wird eingesetzt, um eine hohe Skalierbarkeit zu erreichen. Mit dem ERA-Proxyserver kann der Datenverkehr von den Client-Agenten zusammengefasst werden. Mehrere Agenten können eine Verbindung zum ERA-Proxy herstellen, der den Datenverkehr dann zum ERA-Server weiterleitet. Dies ermöglicht eine Optimierung der Datenbankabfragen. Außerdem kann der ERA-Proxy eine Verbindung zu anderen Proxyservern und dann zum ERA-Server herstellen. Die jeweilige Lösung hängt von der Netzwerkumgebung und Konfiguration ab.

Der ERA-Proxy übernimmt außerdem die passive Verteilung der Konfigurationsdaten (Gruppen, Policies, Tasks usw.) an die Agenten. Diese Weiterleitung erfolgt ohne Eingriff des ERA-Servers.

Der ERA-Proxy (und alle anderen Komponenten) können ausschließlich über Policies vom ERA-Server konfiguriert werden. Dies bedeutet, dass der Agent auf dem ERA-Proxycomputer installiert sein muss, um die Konfiguration vom ERA-Server zum ERA-Proxy zu liefern.

HINWEIS: Eine direkte Verbindung zwischen dem ERA-Server und dem ERA-Proxy ohne Agent ist nicht möglich.



Der **ERA-Proxy** ist ein weiterer Bestandteil von ESET Remote Administrator und dient zwei Zwecken. In einem mittelgroßen Netzwerk oder Unternehmensnetzwerk mit vielen Clients (beispielsweise 10.000 Clients oder mehr) können Sie mit einem ERA-Proxy die Last zwischen mehreren ERA-Proxys verteilen und so den primären ERA-Server entlasten. Sie können den ERA-Proxy außerdem für Verbindungen zu entfernt liegenden Büros mit schwacher Bandbreite einsetzen. Dabei stellt der ERA-Agent des Client nicht direkt eine Verbindung zum ERA-Server her, sondern zum ERA-Proxy, der sich im gleichen lokalen Netzwerk wie der Agent und der Client befindet. Diese Konfiguration ermöglicht eine bessere Kommunikation mit dem entfernt liegenden Büro. Der ERA-Proxy nimmt Verbindungen von allen lokalen ERA-Agenten an, kompiliert die Daten und lädt sie zum primären ERA-Server (oder zu einem anderen ERA-Proxy) hoch. Auf diese Weise ist im Netzwerk Platz für mehr Clients, ohne dass die Leistungsfähigkeit des Netzwerks und der Datenbankabfragen beeinträchtigt wird.

Damit der ERA-Proxy ordnungsgemäß funktioniert, muss auf dem Hostcomputer, auf dem sich der ERA-Proxy befindet, ein ESET-Agent installiert sein, und er muss mit der oberen Ebene (entweder dem ERA-Server oder, sofern vorhanden, dem oberen ERA-Proxy) des Netzwerks verbunden sein.

HINWEIS: Siehe Bereitstellungsszenario mit ERA-Proxy.

1.2.5 Rogue Detection Sensor

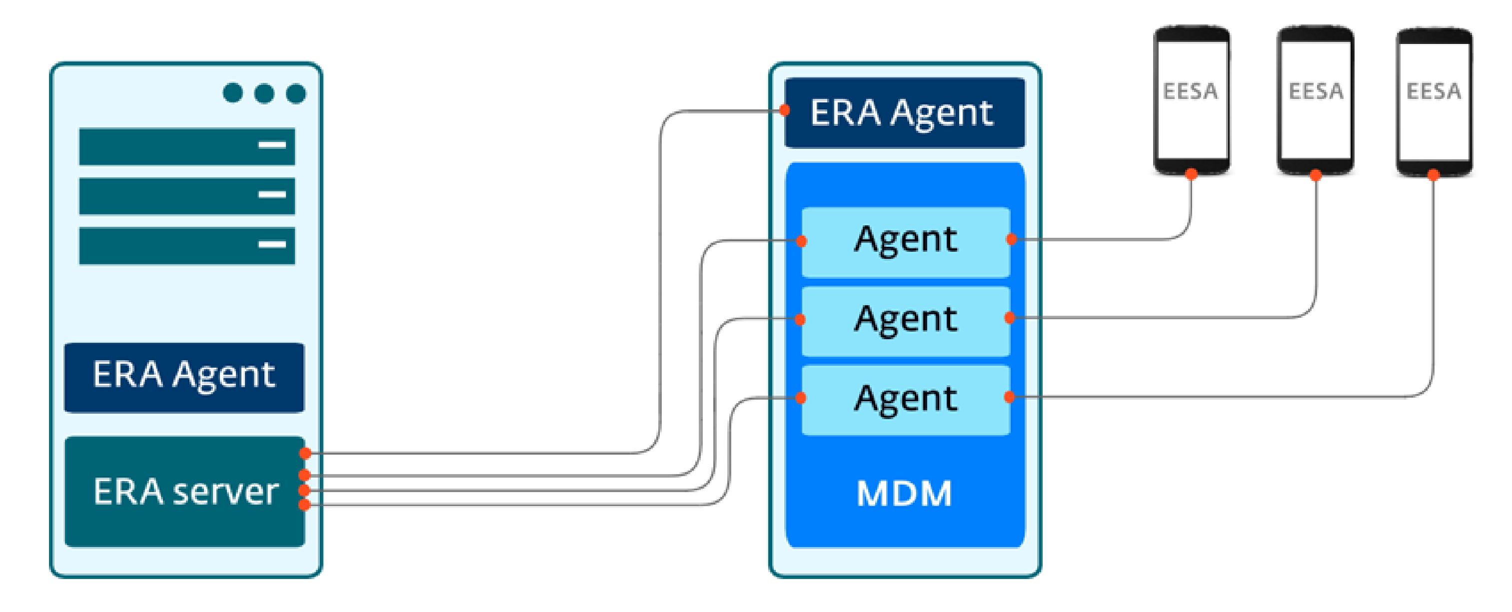
Rogue Detection Sensor (RD Sensor) ist ein Erkennungstool, das Ihr Netzwerk auf unerwünschte Computer durchsucht. Der Sensor ist besonders hilfreich, weil er neue Computer aus ESET Remote Administrator erkennen kann, ohne dass diese gesucht und manuell hinzugefügt werden müssen. Die gefundenen Computer werden sofort erkannt und in einem vordefinierten Bericht gemeldet, sodass Sie diese in bestimmte statische Gruppen verschieben und mit Ihren Verwaltungsaufgaben fortfahren können.

RD Sensor ist ein passives Überwachungstool, das Computer erkennt, die im Netzwerk vorhanden sind, und Informationen über diese Computer an den ERA-Server sendet. Der ERA-Server bewertet dann, ob die im Netzwerk gefundenen PCs dem ERA-Server unbekannt oder ob sie bereits verwaltet sind.

Jeder Computer innerhalb der Netzwerkstruktur (Domäne, LDAP, Windows-Netzwerk) wird über einen Serversynchronisierungstask automatisch der Computerliste auf dem ERA-Server hinzugefügt. Mit dem RD Sensor können auf einfache Weise alle Computer erkannt werden, die nicht in der Domäne oder der Netzwerkstruktur vorhanden sind, und zum ESET Remote Administrator-Server hinzugefügt werden. RD Sensor merkt sich Computer, die bereits erkannt wurden, und sendet nicht zweimal die gleichen Informationen.

1.2.6 Connector für Mobilgeräte

Mit dem **Connector für Mobilgeräte** können Sie Mobilgeräte und ESET Endpoint Security für Android verwalten.



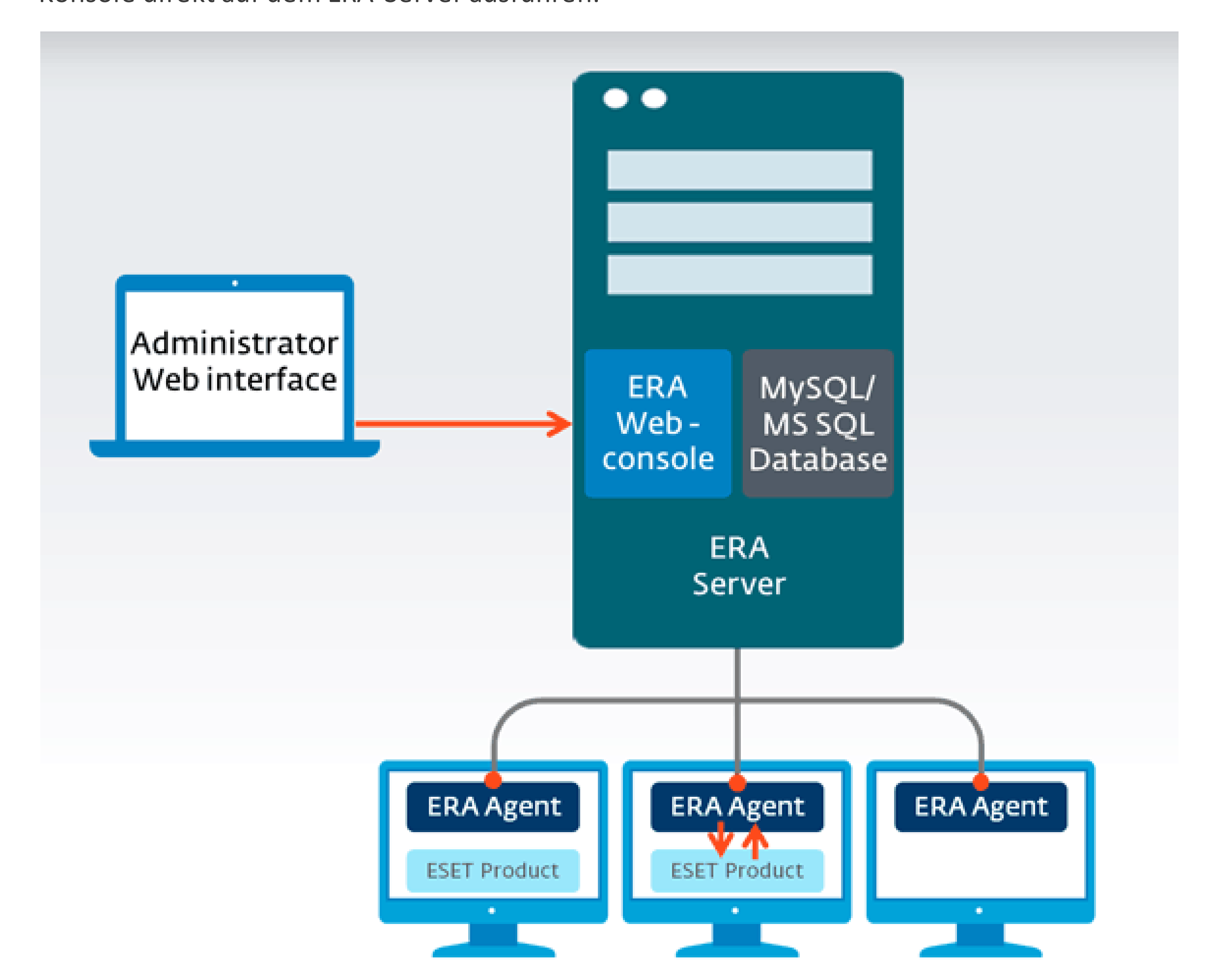
1.2.7 Bereitstellungsszenarien

Die folgenden Kapitel beschreiben Bereitstellungsszenarien für verschiedene Netzwerkumgebungen. Ausführliche Anweisungen finden Sie in den entsprechenden Kapiteln:

- Einzelner Server (kleines Unternehmen)
- Hochverfügbarkeit (Unternehmen)
- Remotezweigstellen mit Proxyservern

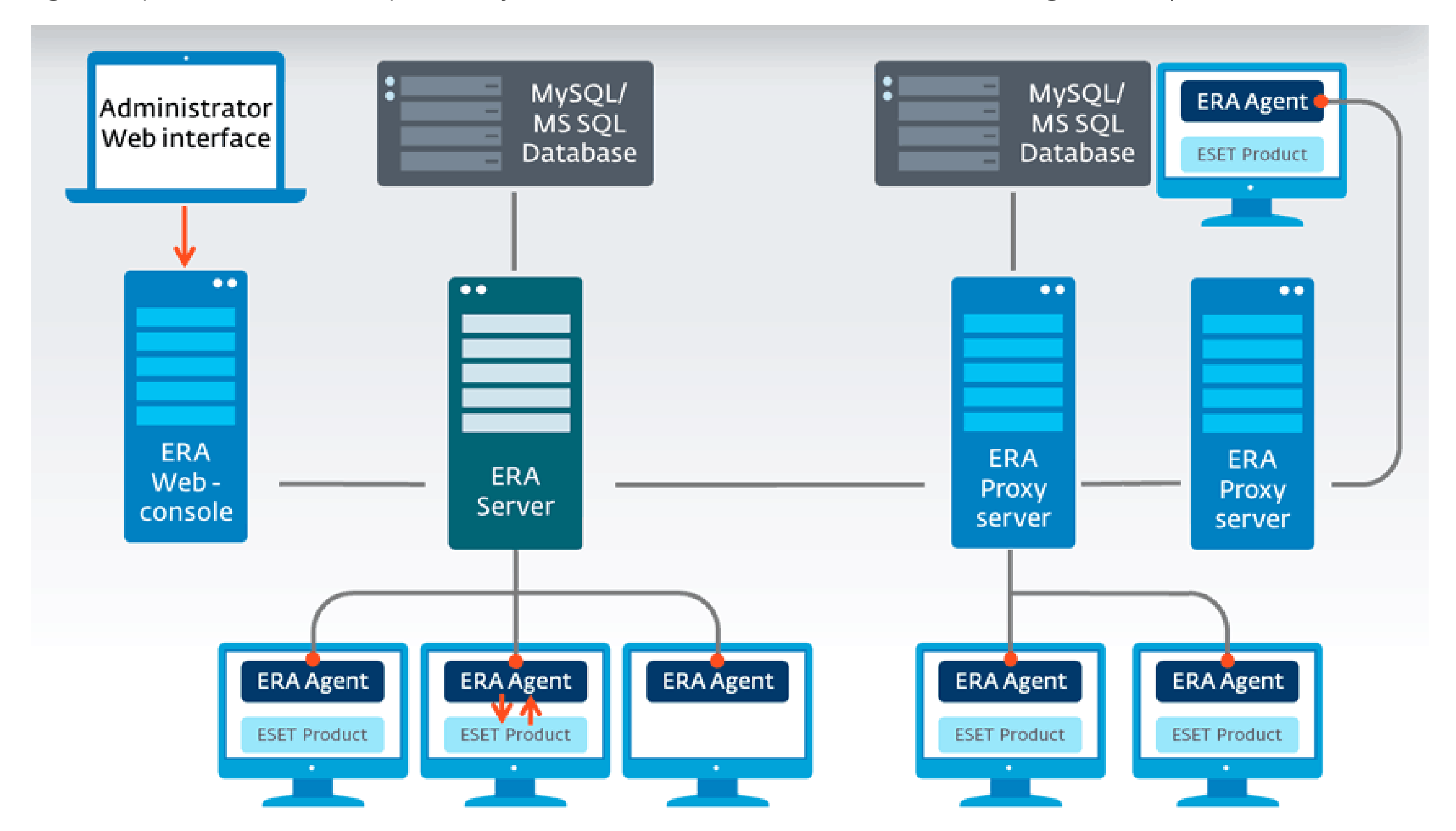
1.2.7.1 Einzelner Server (kleines Unternehmen)

Für die Verwaltung kleiner Netzwerke (mit bis zu 1.000 Clients) reicht üblicherweise ein einziger Computer, auf dem der ERA-Server und alle zugehörigen Komponenten (Webserver, Datenbank usw.) installiert sind. Sie können dies als einzelnen Server oder als Standalone-Installation betrachten. Alle verwalteten Clients stellen direkt über den ERA-Agenten eine Verbindung zum ERA-Server her. Der Administrator kann über einen Webbrowser auf einem beliebigen Computer im Netzwerk eine Verbindung zur ERA Web-Konsole des Servers ausführen oder die Web-Konsole direkt auf dem ERA-Server ausführen.



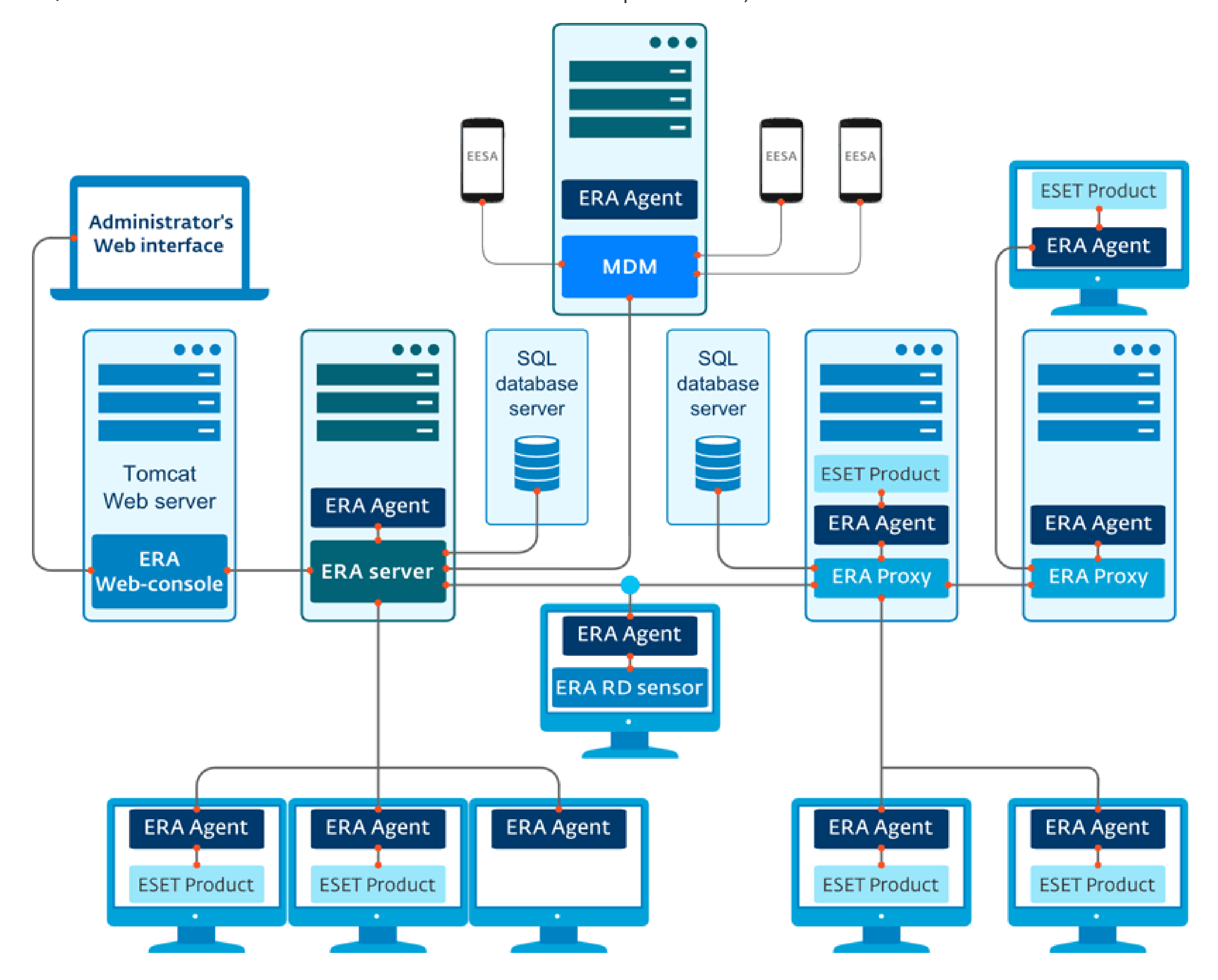
1.2.7.2 Remotezweigstellen mit Proxyservern

In einem mittelgroßen Netzwerk (beispielsweise mit 10.000 Clients) wird ein zusätzlicher Layer aus ERA-Proxyserver hinzugefügt. Die ERA-Agenten sind mit dem ERA-Proxyserver verbunden. Der ERA-Proxyserver kann beispielsweise verwendet werden, wenn die Bandbreite zum Remotestandort (Zweigstelle) gering ist. Die ERA-Agenten (am Remotestandort) können jedoch weiterhin auch direkt eine Verbindung zum Hauptserver herstellen.



1.2.7.3 Hochverfügbarkeit (Unternehmen)

In Unternehmensumgebungen (mit beispielsweise mehr als 100.000 Clients) sollten zusätzliche ERA-Komponenten eingesetzt werden. Eine dieser Komponenten ist der RD Sensor, der das Netzwerk nach neuen Computern durchsucht. Eine weitere Komponente ist eine Ebene aus ERA-Proxyservern. Die ERA-Agenten kommunizieren hierbei über den ERA-Proxyserver. Dies entlastet den Hauptserver, was im Hinblick auf die Leistung von Vorteil ist. Auch in dieser Konfiguration können die ERA-Agenten eine direkte Verbindung zum Hauptserver herstellen. Eine SQL-Datenbank wird ebenfalls in einem Failover-Cluster implementiert, um eine Redundanz zu bieten.



1.2.8 Praktische Bereitstellungsbeispiele

Zur Gewährleistung einer optimalen Leistung empfehlen wird die Verwendung von Microsoft SQL Server als ESET Remote Administrator-Datenbank. ESET Remote Administrator ist auch mit MySQL kompatibel, doch die Verwendung von MySQL kann sich nachteilhaft auf die Systemleistung auswirken, wenn Sie mit großen Datenmengen arbeiten, beispielsweise mit großen Dashboards, vielen Bedrohungen oder vielen Clients. Mit Microsoft SQL Server können Sie mit der gleichen Hardware etwa die 10-fache Anzahl an Clients verarbeiten wie mit MySQL.

Für Testzwecke speichert jeder Client etwa 30 Logs in der Datenbank. Microsoft SQL Server arbeitet mit einem großen RAM-Volumen, um Datenbankdaten im Cache zu speichern. Daher empfehlen wir, mindestens so viel Arbeitsspeicher zur Verfügung zu stellen wie für Microsoft SQL Server auf dem Datenträger vorhanden ist.

Es gibt keine einfache Methode, die Menge der von ESET Remote Administrator verwendeten Ressourcen genau zu berechnen, da dies je nach Netzwerkumgebung variiert. Nachstehend finden Sie einige Testergebnisse für übliche Netzwerkkonfigurationen.

- Testfall: bis zu 5.000 Clients mit Verbindung zum ERA-Server

- Testfall: bis zu 100,000 Clients mit Verbindung zum ERA-Server

Um eine optimale Konfiguration für Ihre Anforderungen zu bestimmen, empfiehlt es sich, einen Test mit einer kleineren Anzahl Clients und weniger leistungsfähiger Hardware auszuführen, und die Systemanforderungen auf Grundlage der erhaltenen Testergebnisse zu extrapolieren.

TESTFALL (5.000 CLIENTS)

Hardware/Software

- Windows Server 2003 R2, x86-Prozessorarchitektur
- Microsoft SQL Server Express 2008 R2
- Intel Core2Duo E8400 mit 3 GHz
- 3 GB RAM
- Seagate Barracuda 7200 RPM, 500 GB, 16 MB Cache, Sata 3,0 Gb/s

Ergebnisse

- Die ERA Web-Konsole antwortet sehr schnell (Antwortzeit unter 5 s)
- Speicherverbrauch:
  - Apache Tomcat 200 MB
  - ERA-Server: 200 MB
  - SQL Server-Datenbank: 1 GB
- Serverreplikationsleistung: 10 Replikationen pro Sekunde
- Datenbankgröße auf dem Datenträger: 1 GB (5.000 Clients mit je 30 Logs in der Datenbank)

In diesem Testfall wurde SQL Server Express 2008 R2 verwendet. Trotz der Einschränkungen (10 GB für die Datenbank, 1 Prozessor, 1 GB RAM) hat sich die Konfiguration als funktions- und leistungsfähig erwiesen. Für Server mit weniger als 5.000 Clients empfiehlt sich die Verwendung von SQL Server Express. Sie können auch zunächst SQL Server Express bereitstellen und auf Microsoft SQL Server (Vollversion) aufrüsten, wenn eine größere Datenbank erforderlich wird. Beachten Sie, dass ältere Express-Versionen (vor 2008 R2) eine Größenbeschränkgung von 4 GB für die Datenbank haben.

Die Serverreplikationsleistung definiert ein Replikationsintervall für die Clients. 10 Replikationen pro Sekunde entsprechen 600 Replikationen pro Minute. Im Idealfall sollte das Replikationsintervall auf allen 5.000 Clients auf 8 Minuten festgelegt werden. Dies würde jedoch einer Last von 100 % auf dem Server ergeben, weshalb in diesem Fall ein längeres Intervall angegeben wird. Für dieses Beispiel empfehlen wir ein Replikationsintervall von 20 bis 30 Minuten.

TESTFALL (100.000 CLIENTS)

Hardware/Software

- Windows Server 2012 R2 Datacenter, x64-Prozessorarchitektur
- Microsoft SQL Server 2012
- Intel Xeon E5-2650v2 mit 2,60 GHz
- 64 GB RAM
- Netzwerkadapter Intel NIC/PRO/1000 PT Dual
- 2x Micron RealSSD C400 SSD-Laufwerke mit 256 GB (eines für System und Software, ein zweites für die SQL Server-Datenbankdateien)

Ergebnisse

- Die Web-Konsole antwortet schnell (Antwortzeit unter 30 s).
- Speicherverbrauch
  - Apache Tomcat: 1 GB
  - ERA-Server: 2 GB
  - SQL Server-Datenbank: 10 GB
- Serverreplikationsleistung: 80 Replikationen pro Sekunde
- Datenbankgröße auf dem Datenträger: 10 GB (100.000 Clients mit je 30 Logs in der Datenbank)

In diesem Testfall wurden alle Komponenten (Apache Tomcat, Web-Konsole, ERA-Server, SQL Server) auf einem Computer installiert, um die Leistungsfähigkeit des ERA-Servers zu testen.

Die große Anzahl Clients verursacht eine größere Speicher- und Datenträgerauslastung durch Microsoft SQL Server. Um eine optimale Leistung zu gewährleisten speichert SQL Server nahezu alle Datenbankinformationen im Cache. Apache Tomcat (Web-Konsole) und der ERA-Server speichern ebenfalls Daten im Cache, was die erhöhte Speicherauslastung in diesem Testfall erklärt.

Der ERA-Server kann 80 Replikationen pro Sekunde (288.000 pro Stunde) liefern. Im Idealfall wäre das Replikationsintervall aller 100.000 Clients etwa 30 Minuten (200.000 Replikationen pro Stunde). Dies würde jedoch eine Serverauslastung von 100 % verursachen, weshalb ein geeignetes Replikationsintervall eher 1 Stunde ist (100.000 Replikationen pro Stunde).

Die Netzwerkauslastung hängt von der Anzahl der Logs ab, die von den Clients erfasst werden. In diesem Test waren dies etwa 20 KB pro Replikation. Bei 80 Replikationen pro Sekunde entspricht dies einer Bandbreite von etwa 1600 KB/s (20 Mbit/s).

In diesem Beispiel wurde ein Szenario mit einem Server verwendet. Durch die Verwendung mehrerer ERA-Proxies (je mehr, desto besser) kann die Prozessor- und Netzwerkauslastung besser verteilt werden. Sowohl die Prozessor- als auch die Netzwerklast werden beim Beantworten der Clientreplikationen verteilt. Besonders mit Clients an entfernten Standorten ist es wichtig, die Netzwerklast zu verteilen. Das Proxy-Replikationsintervall für den Server kann außerhalb der Arbeitszeiten festgelegt werden, wenn eine größere Bandbreite zur Verbindung mit entfernten Standorten verfügbar ist.

1.3 Unterstützte Produkte und Sprachen

Mit ESET Remote Administrator können Sie folgende ESET-Produkte bereitstellen, aktivieren und verwalten:

Verwaltung möglich über ESET Remote Administrator 6	Produktversion	Aktivierungsmethode
ESET Endpoint Security für Windows	6.x und 5.x	6.x - Lizenzschlüssel 5.x - Benutzername/Passwort
ESET Endpoint Antivirus für Windows	6.x und 5.x	6.x - Lizenzschlüssel 5.x - Benutzername/Passwort
ESET Endpoint Security für OS X	6.x	Lizenzschlüssel
ESET Endpoint Antivirus für OS X	6.x	Lizenzschlüssel
ESET Endpoint Security für Android	2.x	Lizenzschlüssel

Verwaltung möglich über ESET Remote Administrator 6	Produktversion	Aktivierungsmethode
ESET File Security für Windows Server	6.x	Lizenzschlüssel
ESET File Security für Microsoft Windows Server	4.5.x	Benutzername/Passwort
ESET NOD32 Antivirus 4 Business Edition für Mac OS X	4.x	Benutzername/Passwort
ESET NOD32 Antivirus 4 Business Edition für Linux Desktop	4.x	Benutzername/Passwort
ESET Mail Security für Microsoft Exchange Server	4.5.x	Benutzername/Passwort
ESET Mail Security für IBM Lotus Domino	4.5.x	Benutzername/Passwort
ESET Security für Microsoft Windows Server Core	4.5.x	Benutzername/Passwort
ESET Security für Microsoft SharePoint Server	4.5.x	Benutzername/Passwort
ESET Security für Kerio	4.5.x	Benutzername/Passwort
ESET NOD32 Antivirus Business Edition	4.2.76	Benutzername/Passwort
ESET Smart Security Business Edition	4.2.76	Benutzername/Passwort

HINWEIS: Ältere Versionen von Windows Server-Produkten als die in der obigen Tabelle angegebenen können momentan nicht mit ESET Remote Administrator verwaltet werden.

Unterstützte Sprachen

Name	Code
English (United States)	de-de
Arabisch (Ägypten)	ar-EG
Chinesisch vereinfacht	zh-CN
Chinesisch traditionell	zh-TW
Kroatisch (Kroatien)	hr-HR
Tschechisch (Tschechische Republik)	cs-CZ
Französisch (Frankreich)	fr-FR
Französisch (Kanada)	fr-FC
Deutsch (Deutschland)	de-DE
Italienisch (Italien)	it-IT
Japanisch (Japan)	ja-JP
Koreanisch (Korea)	ko-KR
Polnisch (Polen)	pl-PL
Portugiesisch (Brasilien)	pt-BR
Russisch (Russland)	ru-RU
Spanisch (Chile)	es-CL
Spanisch (Spanien)	es-ES
Slowakisch (Slowakei)	sk-SK

2. Systemanforderungen

Für die Installation von ESET Remote Administrator müssen bestimmte Hardware-, Datenbank- und Software-Anforderungen erfüllt sein.

2.1 Hardware

Für einen reibungslosen Betrieb von ESET Remote Administrator muss Ihr System die folgenden Hardwareanforderungen erfüllen:

Speicher	4 GB RAM
Festplatte	Mindestens 20 GB freier Speicherplatz
Prozessor	Doppelkernprozessor mit mindestens 2,0 GHz
Netzwerkverbindung	1 GB/s

2.2 Datenbank

ESET Remote Administrator unterstützt zwei Arten Datenbankserver:

- Microsoft SQL Server (inklusive Express- und nicht-Express-Editionen) 2008, 2008 R2, 2012, 2014
- MySQL (Version 5.5 und höher)

Sie können die gewünschte Art des Datenbankservers während der Server- oder Proxy-Installation festlegen. Microsoft SQL Server 2008 R2 Express ist standardmäßig installiert und ist im Installationspaket enthalten. Microsoft SQL Server 2008 R2 Express hat eine Obergrenze für Datenbanken von 10 GB und kann nicht auf einem Domänencontroller installiert werden. Wenn Sie z. B. Microsoft SBS verwenden, empfiehlt es sich, ESET Remote Administrator auf einem anderen Server zu installieren oder während der Installation nicht die SQL Server Express-Komponente auszuwählen (Sie müssen dann zum Ausführen der ERA-Datenbank SQL Server oder MySQL verwenden).

Wenn Sie Microsoft SQL Server verwenden möchten, beachten Sie, dass die früheste unterstützte Version **Microsoft SQL Server 2008** ist. Sie können eine vorhandene Installation von Microsoft SQL Server verwenden, die in Ihrer Umgebung ausgeführt wird, sie muss jedoch die Mindestanforderungen erfüllen.

HINWEIS: ERA-Server und ERA-Proxy arbeiten nicht mit integrierter Sicherung. Wir empfehlen daher dringend, Sicherungen des Datenbankservers zu erstellen, um einen Datenverlust zu vermeiden.

Hardwareanforderungen für den Datenbankserver:

Speicher	1 GB RAM
Festplatte	Mindestens 10 GB freier Speicherplatz
Prozessorgeschwindigkeit	x86-Prozessor: 1,0 GHz x64-Prozessor: 1,4 GHz **Hinweis**: Für eine optimale Leistung wird ein Prozessor mit mindestens 2,0 GHz empfohlen.
Prozessortyp	x86-Prozessor: Pentium III-kompatibler Prozessor oder gleichwertig/besser x64-Prozessor: AMD Opteron, AMD Athlon 64, Intel Xeon mit Intel EM64T-Unterstützung, Intel Pentium IV mit EM64T-Unterstützung

2.3 Unterstützte Betriebssysteme

Die folgenden Abschnitte enthalten Informationen zu den Betriebssystemversionen von Windows, Linux und Mac OS, die von den einzelnen ESET Remote Administrator-Komponenten unterstützt werden.

2.3.1 Windows

Die folgende Tabelle enthält die unterstützten Betriebssysteme der einzelnen ESET Remote Administrator-Komponenten. ERA Server, ERA Proxy und MDM können auch auf Client-Betriebssystemen (*Microsoft Windows 7, 8 , 8.1) installiert werden, jedoch **nur zu Testzwecken**.

Betriebssystem	Server	Agent	Proxy	RD Sensor	MDM
Windows XP x86 SP3		X		X	
Windows XP x64 SP2		X		X	
Windows Vista x86 SP2		X		X	
Windows Vista x64 SP2		X		X	
Windows 7 x86 SP1	*	X	*	X	*
Windows 7 x64 SP1	*	X	*	X	*
Windows 8 x86	*	X	*	X	*
Windows 8 x64	*	X	*	X	*
Windows 8.1 x86	*	X	*	X	*
Windows 8.1 x64	*	X	*	X	*
Windows HomeServer 2003 SP2		X		X	
Windows HomeServer 2011 x64		X		X	
Windows Server 2003 x86 SP2	X	X	X	X	
Windows Server 2003 x64 SP2	X	X	X	X	
Windows Server 2003 x86 R2 SP2	X	X	X	X	
Windows Server 2003 x64 R2 SP2	X	X	X	X	
Windows Server 2008 x64 R2 SP1	X	X	X	X	X
Windows Server 2008 x64 R2 CORE	X	X	X	X	X
Windows Server 2008 x86		X		X	
Windows Server 2008 x86 SP2	X	X	X	X	X
Windows Server 2008 x64		X		X	
Windows Server 2008 x64 SP2	X	X	X	X	X
Windows Server 2012 x64	X	X	X	X	X
Windows Server 2012 x64 CORE	X	X	X	X	X
Windows Server 2012 x64 R2	X	X	X	X	X
Windows Server 2012 x64 R2 CORE	X	X	X	X	X
Microsoft SBS 2003 x86 SP2 **	X	X	X	X	X
Microsoft SBS 2003 x86 R2 **	X	X	X	X	X
Microsoft SBS 2008 x64		X		X	
Microsoft SBS 2008 x64 SP2 **	X	X	X	X	X
Microsoft SBS 2011 x64 Standard	X	X	X	X	X
Microsoft SBS 2011 x64 Essential	X	X	X	X	X

*** ERA-Komponenten auf Client-Betriebssystemen (nur zu Testzwecken).**

**** Die in Microsoft Small Business Server (SBS) enthaltene Version von Microsoft SQL Server Express wird von ESET Remote Administrator** nicht unterstützt. Falls Sie Ihre ERA-Datenbank auf SBS installieren möchten, müssen Sie eine neuere Version von Microsoft SQL Server verwenden. Weitere Informationen und Anweisungen finden Sie unter Installation unter Windows SBS / Essentials**.**

Auf älteren Systemen wie Windows Server 2003 wird die Protokollverschlüsselung auf der Betriebssystemseite möglicherweise nicht vollständig unterstützt. Daher wird TLSv1.0 statt TLSv1.2 verwendet (TLSv1.0 gilt als weniger sicher als aktuellere Versionen). Diese Situation kann auch auftreten, wenn das Betriebssystem TLSv1.2 unterstützt, der Client aber nicht. In diesem Fall erfolgt die Kommunikation über TLS1.0. Wenn Sie eine sicherere Kommunikation benötigen, sollten Sie neuere Betriebssysteme und Clients (Windows Server 2008 R2 oder neuer für Server und Windows Vista oder neuer für Clients) verwenden.

HINWEIS: Sie können auch auf einem Desktop-Betriebssystem installieren und die virtuelle Appliance bereitstellen. Auf diese Weise können Sie ESET Remote Administrator auf Nicht-Server-Betriebssystemen ohne ESXi ausführen.

2.3.2 Linux

Betriebssystem	Server	Agent	Proxy	RD Sensor	MDM
Ubuntu 12.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x86 Server	X	X	X	X	X
Ubuntu 12.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 12.04 LTS x64 Server	X	X	X	X	X
Ubuntu 14.04 LTS x86 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x86 Server	X	X	X	X	X
Ubuntu 14.04 LTS x64 Desktop	X	X	X	X	X
Ubuntu 14.04 LTS x64 Server	X	X	X	X	X
RHEL 5 x86		X			
RHEL 5 x64		X			
RHEL Server 6 x86	X	X	X	X	X
RHEL Server 6 x64	X	X	X	X	X
RHEL Server 7 x86	X	X	X	X	X
RHEL Server 7 x64	X	X	X	X	X
CentOS 5 x86		X			
CentOS 5 x64		X			
CentOS 6 x86	X	X	X	X	X
CentOS 6 x64	X	X	X	X	X
CentOS 7 x86	X	X	X	X	X
CentOS 7 x64	X	X	X	X	X
SLED 11 x86	X	X	X	X	X
SLED 11 x64	X	X	X	X	X
SLES 11 x86	X	X	X	X	X
SLES 11 x64	X	X	X	X	X
OpenSUSE 13 x86	X	X	X	X	X
OpenSUSE 13 x64	X	X	X	X	X
Debian 7 x86	X	X	X	X	X
Debian 7 x64	X	X	X	X	X
Fedora 19 x86	X	X	X	X	X
Fedora 19 x64	X	X	X	X	X
Fedora 20 x86	X	X	X	X	X
Fedora 20 x64	X	X	X	X	X

2.3.3 OS X

Betriebssystem	Agent
OS X 10.7 Lion	X
OS X 10.8 Mountain Lion	X
OS X 10.9 Mavericks	X
OS X 10.10 Yosemite	X

HINWEIS: OS X wird nur als Client unterstützt. Der ERA-Server kann nicht auf OS X-Systemen installiert werden.

2.4 Verwendete Ports

Die nachstehenden Tabellen enthalten eine Liste aller Netzwerkkommunikationsports, die verwendet werden, wenn ESET Remote Administrator mit den Komponenten in Ihrer Infrastruktur installiert ist. Die sonstige Kommunikation erfolgt über die nativen Prozesse des Betriebssystems (zum Beispiel NetBIOS über TCP/IP).

ERA-Server:

Protokoll	Port	Verwendung	Beschreibung
TCP	2222	ERA Server-Überwachung	Kommunikation zwischen Clients und ERA Server
TCP	2223	ERA Server -Überwachung	Kommunikation zwischen ERA Web Console und ERA Server für die unterstützte Installation.
UDP	1237	Übertragung	Aktivierungsaufruf

ERA-Web-Konsole:

Protokoll	Port	Verwendung	Beschreibung
TCP	2223		Web-Konsole
TCP	443		HTTP SSL Web-Konsole

ERA-Proxy:

Protokoll	Port	Verwendung	Beschreibung
TCP	3128		HTTP-Proxy (Update-Cache)
TCP	2222		Proxy

ERA-Agent:

Protokoll	Port	Verwendung	Beschreibung
TCP	139	Zielport aus Sicht von ERA Server	Verwenden der Freigabe ADMIN$
TCP	445	Zielport aus Sicht von ERA Server	Direktzugriff auf freigegebene Ressourcen mit TCP/IP während der Remote-Installation (Alternative zu TCP 139)
UDP	137	Zielport aus Sicht von ERA Server	Namensauflösung während der Remote-Installation
UDP	138	Zielport aus Sicht von ERA Server	Durchsuchen während der Remote-Installation

Connector für Mobilgeräte:

Protokoll	Port	Verwendung	Beschreibung
TCP	9980	Mobilgeräteregistrierung	Registrierungsport
TCP	9981	Kommunikation mit ERA	Connector für Mobilgeräte stellt Verbindung zum ERA-Server her

Die vordefinierten Ports 2222 und 2223 können geändert werden, wenn sie bereits von anderen Anwendungen genutzt werden.

HINWEIS: Die oben genannten Ports dürfen nicht von anderen Awendungen verwendet werden. Andernfalls können Probleme auftreten.

HINWEIS: Vergewissern Sie sich, dass die Firewall(s) in Ihrem Netzwerk so konfiguriert sind, dass die Kommunikation über die oben genannten Ports zugelassen wird.

3. Installationsprozedur

Für die Installation von ESET Remote Administrator stehen verschiedene Methoden zur Verfügung. Wählen Sie die Installationsart aus, die sich am besten für Ihre Anforderungen und Ihre Umgebung eignet. Die einfachste Methode ist die Verwendung des ESET Remote Administrator(ERA)-Installationspakets (All-in-One-Installation), mit dem Sie ESET Remote Administrator und alle Komponenten auf einem einzigen Computer installieren können. Die Komponenteninstallation ermöglicht die Installation einzelner Komponenten von ESET Remote Administrator auf verschiedenen Computern. So können Sie Ihre Installation besser an besondere Anforderungen anpassen - jede Komponente kann auf einem beliebigem Computer installiert werden, sofern dieser die Systemvoraussetzungen erfüllt. Die Bereitstellung als virtuelle Appliance ermöglicht das Ausführen von ERA in einer virtuellen Umgebung.

Die Installationsprogramme für ESET Remote Administrator sind in verschiedenen Formen verfügbar. Sie können Sie im Downloadbereich der ESET-Website unter **Remote Management** herunterladen (klicken Sie auf das Symbol „+“, um die Kategorie auszuklappen). Hier können Sie folgende Formen herunterladen:

- ERA-Installationspaket im komprimierten Format
- Getrennte Installationsprogramme für jede Komponente
- Virtuelle Appliance (OVA-Datei)
- Ein ISO-Abbild mit allen Installationsprogrammen von ESET Remote Administrator (einschließlich der oben genannten)

Befolgen Sie diese Schritte, um ESET Remote Administrator zu installieren:

1. Vergewissern Sie sich, dass alle Anforderungen erfüllt sind.

2. Wählen Sie entweder die Paketinstallation (All-in-One ERA-Installationspaket) oder die Komponenteninstallation für Ihr Windows- oder Linux-Betriebssystem aus. Alternativ können Sie die virtuelle Appliance verwenden, indem Sie eine OVF-Datei bereitstellen.

3. Laden Sie das geeignete Installationsprogramm herunter: entweder das Installationspaket für die Paketinstallation oder separate Installationsprogramme für jede Komponente, die Sie installieren möchten. Sie können auch eine OVA-Datei für eine virtuelle Appliance oder ein ISO-Abbild herunterladen, das alle Installationsprogramme von ESET Remote Administrator enthält.

4. Befolgen Sie zum Ausführen der Installation die Anweisungen, die in den nächsten Kapitel enthalten sind.

5. Installieren Sie ggf. optionale Komponenten (ERA-Proxyserver, RD Sensor, Connector für Mobilgeräte)

Nach der Installation können Sie über die ERA Web-Konsole eine Verbindung zum ERA-Server herstellen und erste Schritte zur Konfiguration ausführen, um mit der Verwendung von ESET Remote Administrator zu beginnen.

3.1 Paketinstallation

Die Paketinstallation oder „Bootstrapper“ (All-in-One-Installation) ist nur für Windows-Betriebssysteme verfügbar. Sie stellt eine komfortable Methode zur Installation aller ERA-Komponenten über einen einfachen Installationsassistenten dar. Beim Ausführen des Installationspaket werden zwei Optionen angezeigt:

- Remote Administrator Server-Installation
- Remote Administrator Proxy-Installation

Remote Administrator Server-Installation

Führen Sie die hier beschriebenen Anweisungen aus, sehen Sie sich unser Anleitungsvideo in der Knowledgebase oder besuchen Sie unseren Knowledgebase-Artikel für illustrierte und ausführliche Anweisungen für die Installation mithilfe der All-in-One-Installation.

1. Doppelklicken Sie auf das Installationspaket, um die Installation zu starten. Wählen Sie **Remote Administrator Server** aus.

HINWEIS: Wenn Sie ERA in einer Umgebung mit Failover-Cluster installieren möchten, müssen Sie eine Komponenteninstallation ausführen.

2. Wählen Sie die Komponenten aus, die Sie installieren möchten. Wenn Sie keinen Datenbankserver haben, können Sie Microsoft SQL Server 2008 R2 Express installieren. Dies ist im Installationspaket enthalten. Beachten Sie, dass die Datenbankgröße bei Microsoft SQL Server 2008 R2 Express auf 10 GB beschränkt ist. Mit der Paketinstallationsmethode können Sie auch die ERA Web-Konsole, den Connector für Mobilgeräte, den Apache HTTP Proxy sowie den RD Sensor installieren.

3. Geben Sie einen gültigen Lizenzschlüssel ein oder wählen Sie **Später aktivieren** aus.

4. Wenn Sie eine SQL Express-Datenbank verwenden, wird die Verbindung zur Datenbank überprüft. Sie werden zur Eingabe eines Passworts für die ERA Web-Konsole (Schritt 8) und eines Zertifikatpassworts (Schritt 10) aufgefordert.

5. Wenn Sie ein anderes Datenbanksystem verwenden: Wählen Sie **Dienstbenutzerkonto** aus. Mit diesem Konto wird der ESET Remote Administrator-Serverdienst ausgeführt. Folgende Optionen stehen zur Verfügung:

   a. Netzwerkdienstkonto
   b. Bestimmter Benutzer: DOMÄNE/BENUTZERNAME

6. Stellen Sie eine Verbindung zu einer Datenbank her. Hier werden alle Daten gespeichert, vom Web-Konsolen-Passwort zu den Logs der Clientcomputer.

   a. Datenbank: MySQL/MS SQL
   b. ODBC-Treiber: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/SQL Server
   c. Hostname: Hostname oder IP-Adresse des Datenbankservers
   d. Port, der für die Verbindung zum Server verwendet wird
   e. Benutzername/Passwort des Datenbankadministrators

In diesem Schritt wird die Verbindung zur Datenbank überprüft. Wenn die Verbindung erfolgreich ist, können Sie zum nächsten Schritt fortfahren.

7. Wählen Sie einen Benutzer für ESET Remote Administrator aus, der zum Zugriff auf die Datenbank berechtigt ist. Sie können einen vorhandenen Benutzer verwenden oder einen neuen Benutzer erstellen.

8. Geben Sie ein Passwort für den Zugriff auf die **Web-Konsole** ein.

9. ESET Remote Administrator verwendet Zertifikate für die Client-Server-Kommunikation. Wählen Sie entweder Ihre eigenen Zertifikate aus oder lassen Sie vom **Server** neue Zertifikate erstellen.

10. Legen Sie ein Passwort für das **Agenten**zertifikat fest. Merken Sie sich das Passwort gut. Um eine Zertifizierungsstelle für ESET Remote Administrator zu erstellen, klicken Sie auf **Weiter**. Optional können Sie zusätzliche Informationen zum Zertifikat angeben (keine Pflichtangabe). Sie können das Feld **Passwort der Behörde** leer lassen. Falls Sie jedoch ein Passwort eingeben, **merken Sie es sich gut**.

11. Klicken Sie auf **Installieren**, um den ERA-Server zu installieren.

12. Klicken Sie nach Abschluss der Installation auf den im Einrichtungsassistenten angezeigten Link, um die Web-Konsole zu öffnen (wir empfehlen, ein Lesezeichen für diese URL anzulegen), und klicken Sie auf **Fertig stellen**.

HINWEIS: Wenn die Installation mit dem Fehler 2068052081 beendet wird, beachten Sie die Lösungshinweise in den Häufig gestellten Fragen.

Remote Administrator Proxy-Installation

1. Starten Sie das Installationspaket. Wählen Sie **Remote Administrator Proxy** aus.

2. Wählen Sie die Komponenten aus, die Sie installieren möchten. Wenn Sie keinen Datenbankserver haben, können Sie Microsoft SQL Server 2008 R2 Express installieren. Dies ist im Installationspaket enthalten. Beachten Sie, dass die Datenbankgröße bei Microsoft SQL Server 2008 R2 Express auf 10 GB beschränkt ist. Mit der Paketinstallationsmethode können Sie auch RD Sensor installieren.

3. Stellen Sie eine Verbindung zu einer Datenbank her:

   a. Datenbank: MySQL/MS SQL
   b. ODBC-Treiber: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/SQL Server
   c. Hostname: Hostname oder IP-Adresse des Datenbankservers
   d. Port für die Verbindung zum Server
   e. Benutzername/Passwort des Datenbankadministrators

In diesem Schritt wird die Verbindung zur Datenbank überprüft. Wenn die Verbindung erfolgreich ist, können Sie zum nächsten Schritt fortfahren.

4. Wählen Sie einen Kommunikationsport für den Proxyserver aus. Standardmäßig wird Port 2222 verwendet.

5. Konfigurieren Sie die Proxyverbindung zu ESET Remote Administrator. Geben Sie einen Enter a **Server-Hostnamen** (Hostname/IP-Adresse des Servers) und den **Serverport** (2222) an.

6. Wählen Sie ein Peerzertifikat und ein Passwort für das Zertifikat aus. Fügen Sie optional eine Zertifizierungsstelle hinzu. Dies ist nur für nicht signierte Zertifikate erforderlich.

7. Optional können Sie einen Ordner auswählen, in dem der Proxy installiert wird. Klicken Sie dann auf „Installieren".

8. Der Agent wird zusätzliche zum Proxy installiert.

3.1.1 Installation unter Windows SBS / Essentials

Stellen Sie sicher, dass alle Anforderungen erfüllt sind und dass Sie ein unterstütztes Betriebssystem verwenden.

HINWEIS: Manche ältere Microsoft SBS-Versionen enthalten Versionen von Microsoft SQL Server Express, die von ESET Remote Administrator nicht unterstützt werden:

Microsoft SBS 2003 x86 SP2
Microsoft SBS 2003 x86 R2
Microsoft SBS 2008 x64 SP2

Falls Sie eine dieser Versionen von Windows Small Business Server verwenden und die ERA-Datenbank auf Microsoft SBS installieren möchten, müssen Sie eine neuere Version von Microsoft SQL Server Express verwenden.

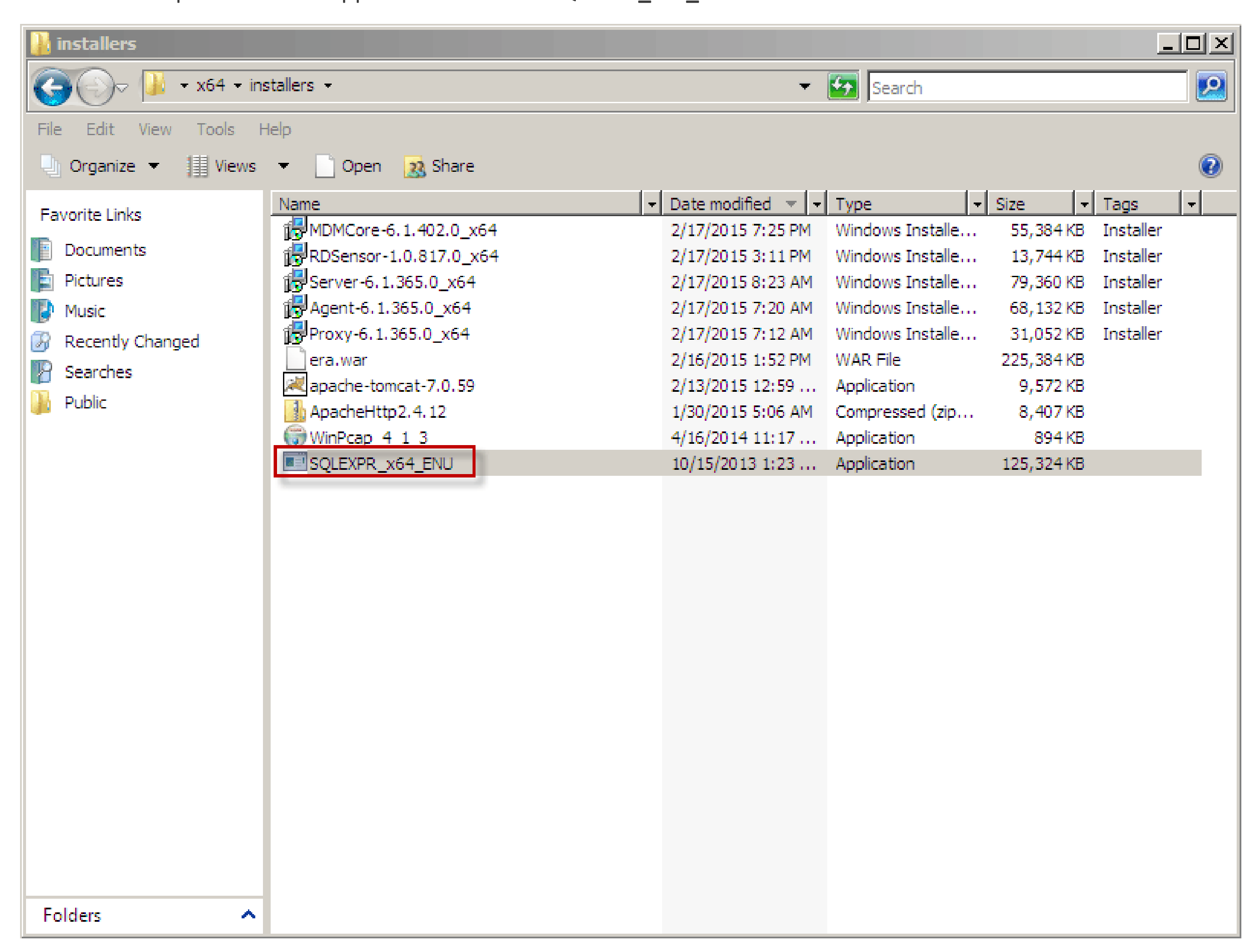
- Führen Sie die folgenden Schritte aus, falls Sie Microsoft SQL Express auf Ihrem SBS installiert haben.

- Falls Sie Microsoft SQL Express auf Ihrem SBS installiert haben, es aber nicht verwenden, deinstallieren Sie Microsoft SQL Express zunächst und führen Sie anschließend die folgenden Schritte aus.

- Falls Sie die mit SBS ausgelieferte Version von Microsoft SQL Server Express verwenden, migrieren Sie Ihre Datenbank auf eine SQL Express-Version, die mit dem ERA-Server kompatibel ist. Sichern Sie dazu zunächst Ihre Datenbanken, deinstallieren Sie Ihre bisherige Installation von Microsoft SQL Server Express und führen Sie die folgenden Schritte aus, um eine kompatible Version von Microsoft SQL Server Express zu installieren und die Datenbanken ggf. wiederherzustellen.

1. Laden Sie das ERA-Installationspaket in gezippter Form im [Downloadbereich] der ESET-Website unter **Remote Management** herunter (klicken Sie auf das Symbol „+“, um die Kategorie zu erweitern).

2. Entzippen Sie die im ersten Schritt heruntergeladene Installationsdatei, öffnen Sie den Ordner mit den Installationspaketen und doppelklicken Sie auf **SQLEXPR_x64_ENU**.



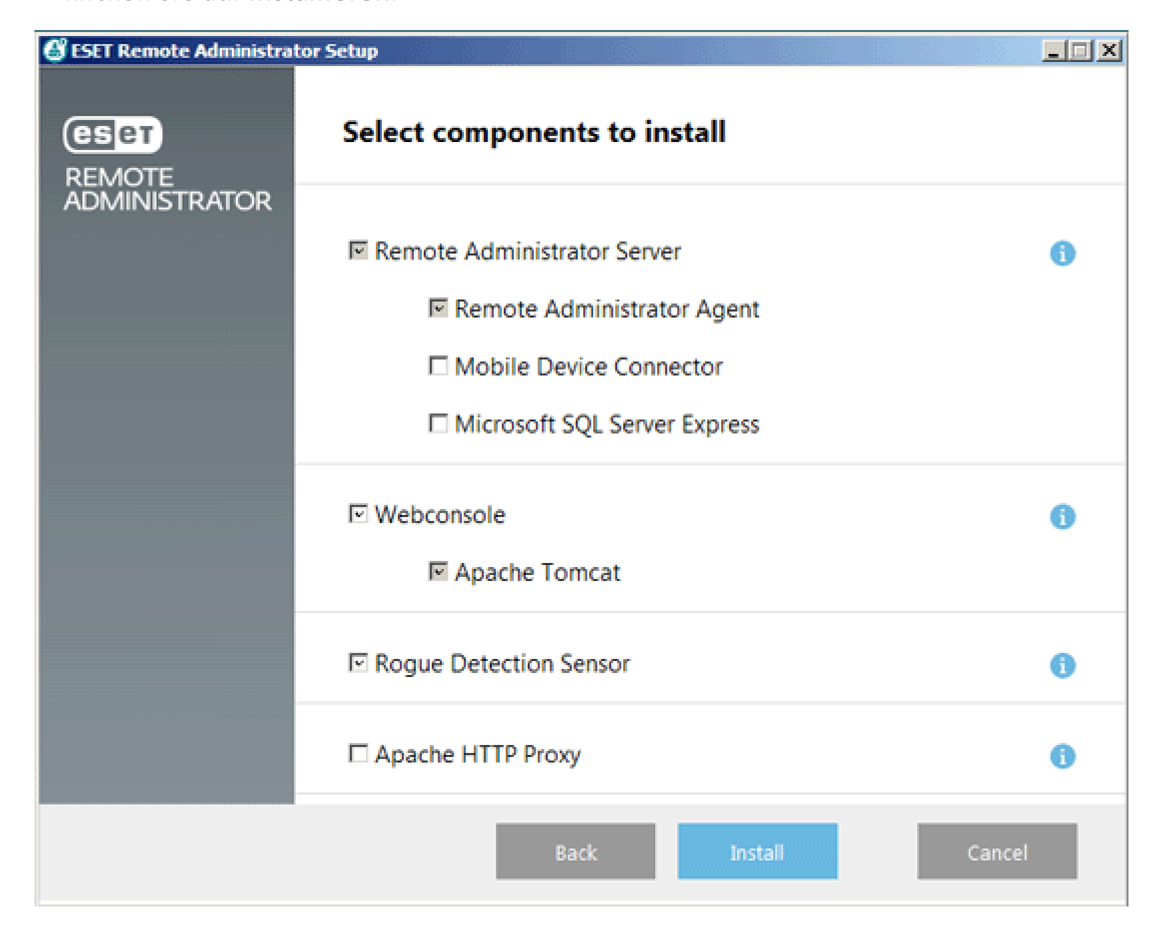
- Das Installations-Center wird gestartet. Klicken Sie auf **Neue Installation oder Features zu vorhandener Installation hinzufügen**, um den Installations-Assistenten zu starten.

HINWEIS: Setzen Sie den Authentifizierungsmodus in Schritt 8 des [Installationsprozesses] auf **Gemischter Modus (SQL Server-Authentifizierung und Windows-Authentifizierung)**.

HINWEIS: Sie müssen [TCP/IP-Verbindungen zum SQL Server erlauben], um den ERA-Server auf SBS zu installieren.

3. Installieren Sie ESET Remote Administrator, indem Sie **Setup.exe** ausführen.

4. Wählen Sie die gewünschten Komponenten aus, deaktivieren Sie die Option Microsoft SQL Server Express und klicken Sie auf **Installieren**.



3.2 Datenbank

ESET Remote Administrator verwendet eine Datenbank zur Speicherung von Clientdaten. In den folgenden Abschnitten werden Installation, Sich, Upgrade und Migration der ERA-Server-/Proxy-Datenbank beschrieben:

- Prüfen Sie die Datenbankkompatibilität und die Systemanforderungen für den ERA-Server.
- Für den Fall, dass Sie keine Datenbank für den ERA-Server konfiguriert haben, ist **Microsoft SQL Server Express** im Installationsprogramm enthalten.
- Falls Sie Microsoft Small Business Server (SBS) oder Essentials verwenden, sollten Sie sicherstellen, dass alle Anforderungen erfüllt sind und dass Sie ein unterstütztes Betriebssystem verwenden. Wenn alle Anforderungen erfüllt sind, folgen Sie den Installationshinweisen für Windows SBS / Essentials, um ERA auf diesen Betriebssystemen zu installieren.
- Falls Sie Microsoft SQL Server auf Ihrem System installiert haben, prüfen Sie die Anforderungen, um sicherzustellen, dass Ihre Version von Microsoft SQL Server von ESET Remote Administrator unterstützt wird. Falls Ihre Version von Microsoft SQL Server nicht unterstützt wird, führen Sie ein Upgrade auf eine unterstützte Version von SQL Server durch.

3.2.1 Datenbankserver-Sicherung

Alle Informationen und Einstellungen von ESET Remote Administrator werden in einer Datenbank gespeichert. Wir empfehlen, die Datenbank regelmäßig zu sichern, um einen Datenverlust zu vermeiden. Weitere Informationen finden Sie im Abschnitt für den verwendeten Datenbanktyp:

- MySQL
- SQL Server

Die Sicherung kann auch für eine Migration von ESET Remote Administrator auf einen neuen Server verwendet werden.

Hier finden Sie Anweisungen zum Wiederherstellen einer Datenbanksicherung:

- MySQL
- SQL Server

3.2.2 Datenbankserver-Upgrade

Führen Sie die folgenden Anweisungen aus, um eine vorhandene Microsoft SQL Server-Instanz# auf eine neuere Version zu aktualisieren, die als Datenbank für den ERA-Server oder den ERA-Proxy verwendet werden kann:

1. **Beenden** Sie alle laufenden ERA-Server- bzw. ERA-Proxy-Dienste, die sich mit dem Server verbinden, den Sie aktualisieren werden. Beenden Sie außerdem alle sonstigen Anwendungen, die sich mit Ihrer Microsoft SQL Server-Instanz verbinden.
2. Sichern Sie alle relevanten Datenbanken an einem sicheren Ort, bevor Sie fortfahren.
3. Führen Sie das Upgrade des Datenbankservers gemäß der Anweisungen des Herstellers durch.
4. **Starten** Sie alle ERA-Server- und/oder ERA-Proxy-Dienste und öffnen Sie deren Trace-Logs, um sicherzustellen, dass die Datenbankverbindung korrekt funktioniert.

Auf den folgenden Webseiten finden Sie weitere Informationen für Ihre spezielle Datenbank:

- SQL Server-Upgrade https://msdn.microsoft.com/en-us/library/bb677622.aspx (klicken Sie auf **Andere Versionen** für Upgrade-Anweisungen auf eine bestimmte SQL Server-Version)
- MySQL Server-Upgrade (auf Version 5.6) http://dev.mysql.com/doc/refman/5.6/en/upgrading.html

3.2.3 ERA-Datenbankmigration

Klicken Sie auf den entsprechenden Link für Anweisungen zur Migration der ERA-Server- bzw. ERA-Proxy-Datenbank zwischen unterschiedlichen SQL Server-Instanzen (gilt ebenfalls für die Migration zwischen unterschiedlichen SQL Server-Versionen oder für die Migration auf einen SQL Server auf einem anderen Computer):

- Migrationsprozess für SQL Server
- Migrationsprozess für MySQL Server

3.2.3.1 Migrationsprozess für SQL Server

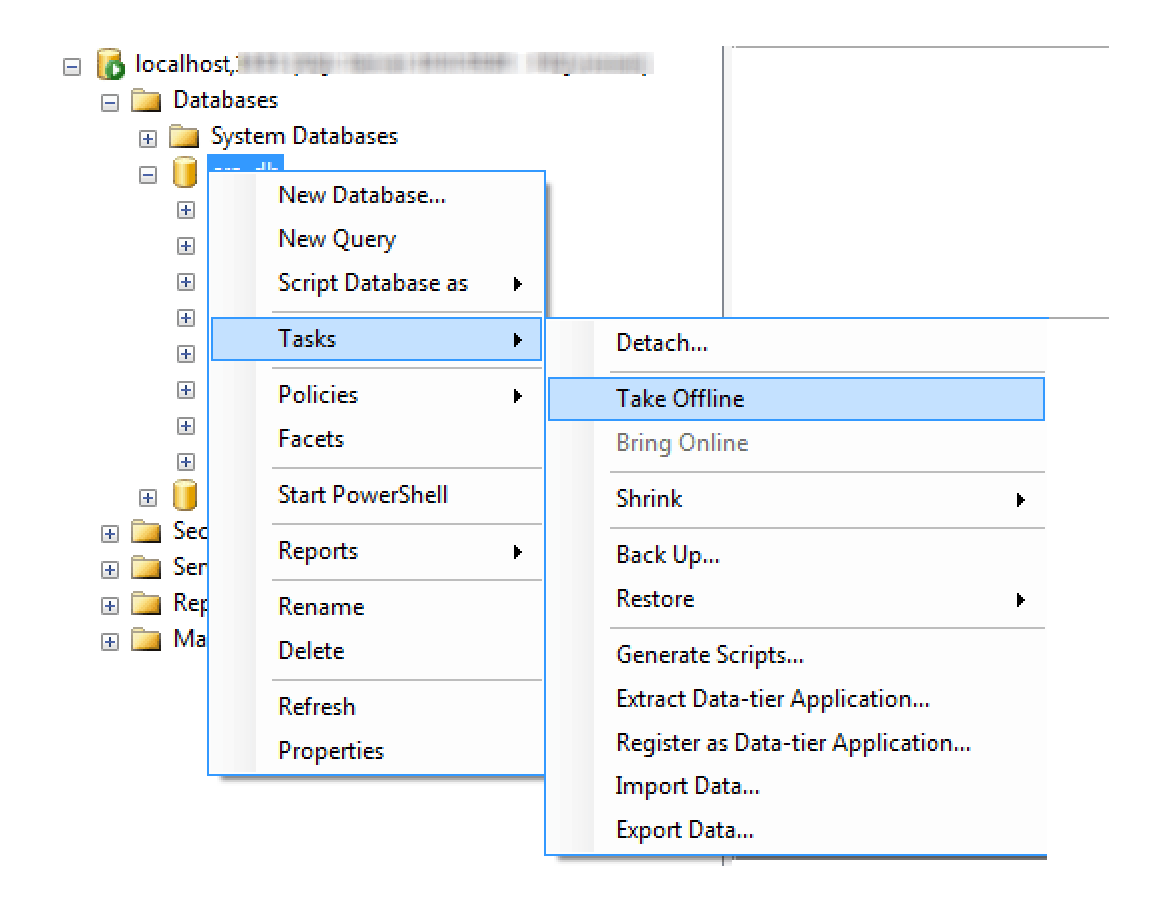
Für **Microsoft SQL Server** und **Microsoft SQL Server Express** wird jeweils derselbe Migrationsprozess verwendet.

Weitere Informationen finden Sie im folgenden Artikel der Microsoft-Knowledgebase: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

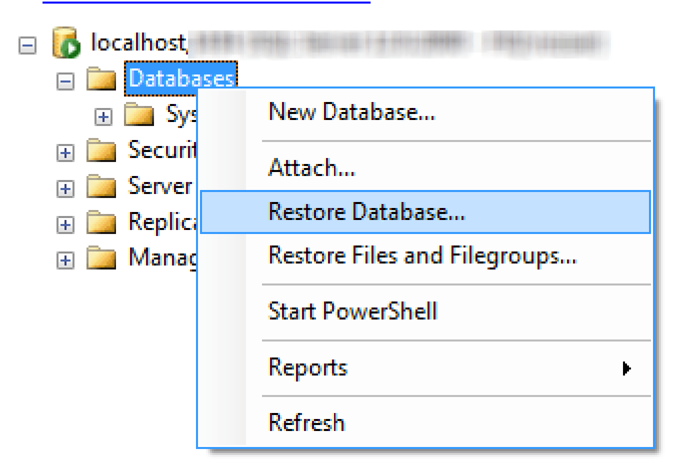
- **Voraussetzungen:**
  - SQL Server-Quell- und Zielinstanzen müssen installiert sein. Diese Instanzen können sich auf unterschiedlichen Computern befinden.
  - Die SQL Server-Zielinstanz muss mindestens dieselbe Version wie die Quellinstanz haben. **Herabstufung wird nicht unterstützt!**
  - **SQL Server Management Studio** muss installiert sein. Wenn sich die SQL Server-Instanzen auf unterschiedlichen Computern befinden, muss Management Studio auf beiden Computern vorhanden sein.

- **Migration:**

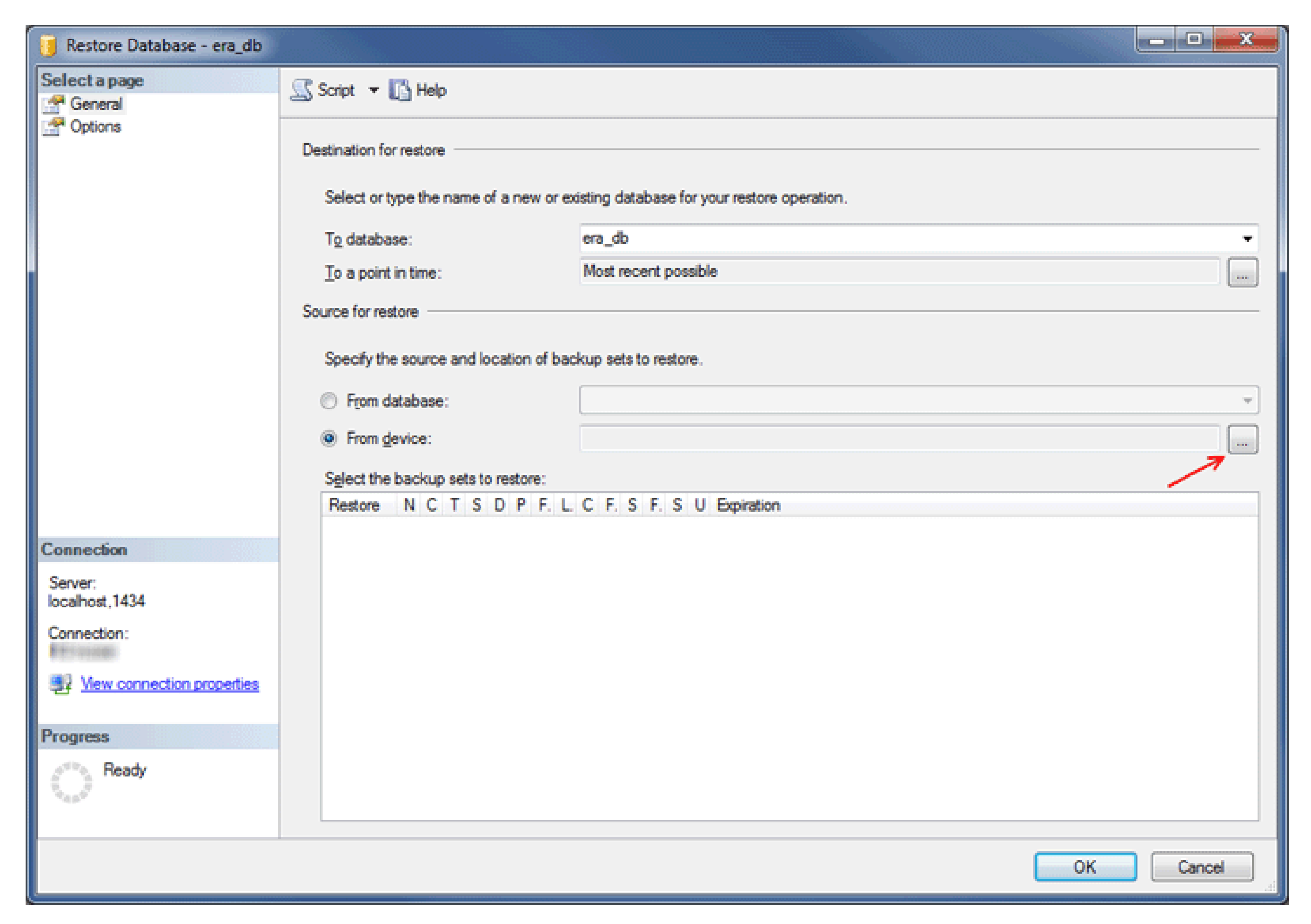
1. **Beenden** Sie den ERA Server- bzw. ERA Proxy-Dienst.
2. Melden Sie sich über SQL Server Management Studio bei der SQL Server-Quellinstanz an.
3. **Erstellen Sie** eine vollständige Datenbanksicherung der zu migrierenden Datenbank. Wir empfehlen die Angabe eines neuen Namens für den Sicherungssatz. Falls der Sicherungssatz bereits verwendet wurde, kann es ansonsten passieren, dass die neue Sicherung daran angehängt wird, was wiederum zu einer unnötig großen Sicherungsdatei führt.
4. Nehmen Sie die Quelldatenbank vom Netz. Wählen Sie dazu **Tasks** > **Offline nehmen** aus.



5. **Kopieren** Sie die in Schritt 3 erstellte Sicherungsdatei (.bak) an einen von der SQL Server-Zielinstanz aus erreichbaren Ort. Möglicherweise müssen Sie die Zugriffsrechte für die Datenbank-Sicherungsdatei bearbeiten.
6. **Stellen Sie die** Quelldatenbank wieder online, aber **starten Sie ERA Server noch nicht!**
7. Melden Sie sich über SQL Server Management Studio bei der SQL Server-Zielinstanz an.
8. Stellen Sie Ihre Datenbank auf der SQL Server-Zielinstanz wieder her.



9. Geben Sie im Feld Zieldatenbank einen Namen für Ihre neue Datenbank ein. Sie können auch den Namen Ihrer alten Datenbank verwenden.
10. Wählen Sie **Von Gerät** unter **Geben Sie die Quelle und den Speicherort der wiederherzustellenden Sicherungssätze an** aus und klicken Sie auf **...** .

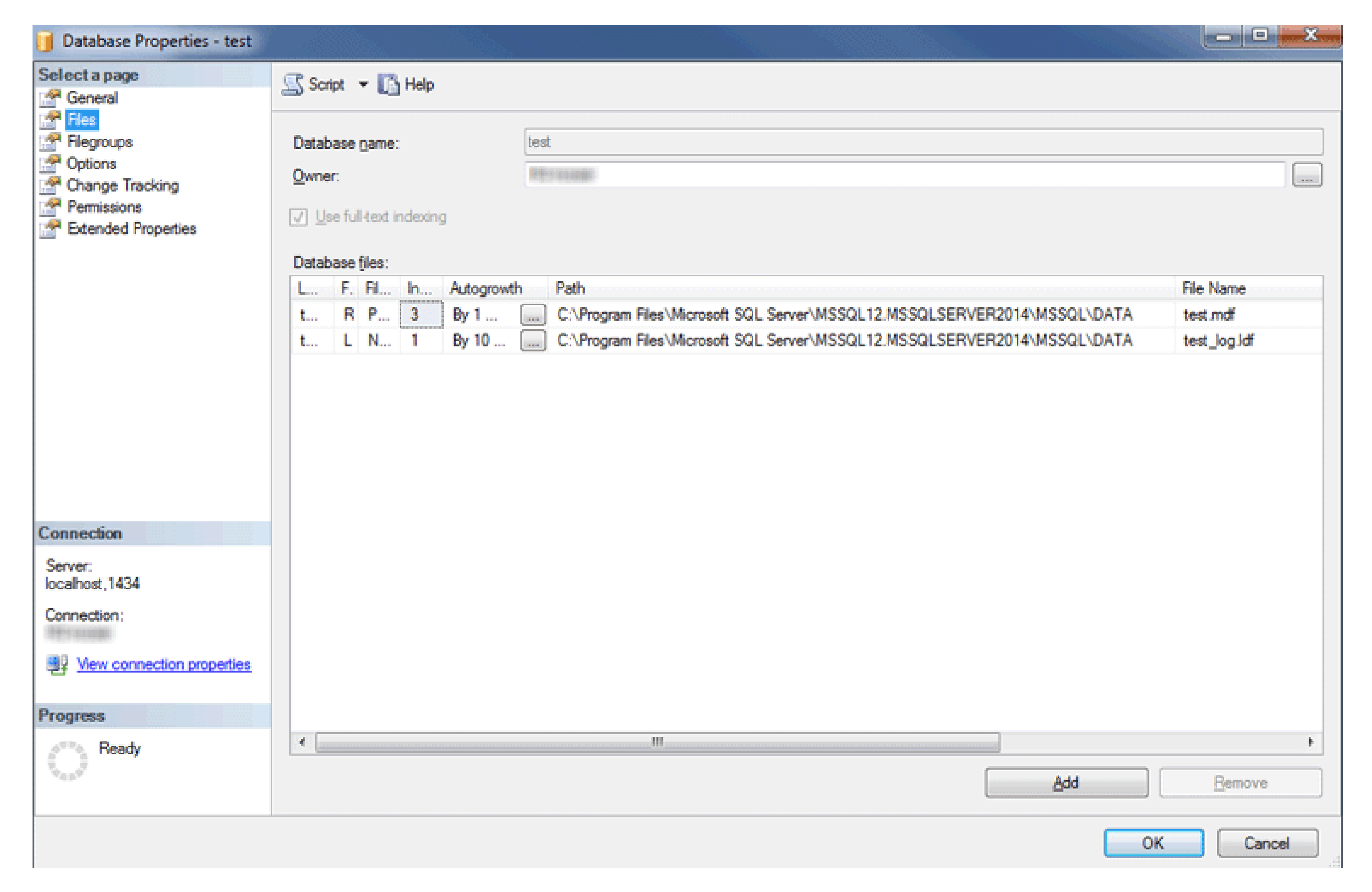


11.Klicken Sie auf **Hinzufügen**, navigieren Sie zu Ihrer Sicherungsdatei und öffnen Sie die Datei.

12. Wählen Sie die aktuellste Sicherung für die Wiederherstellung aus (der Sicherungssatz kann mehrere Sicherungen enthalten).

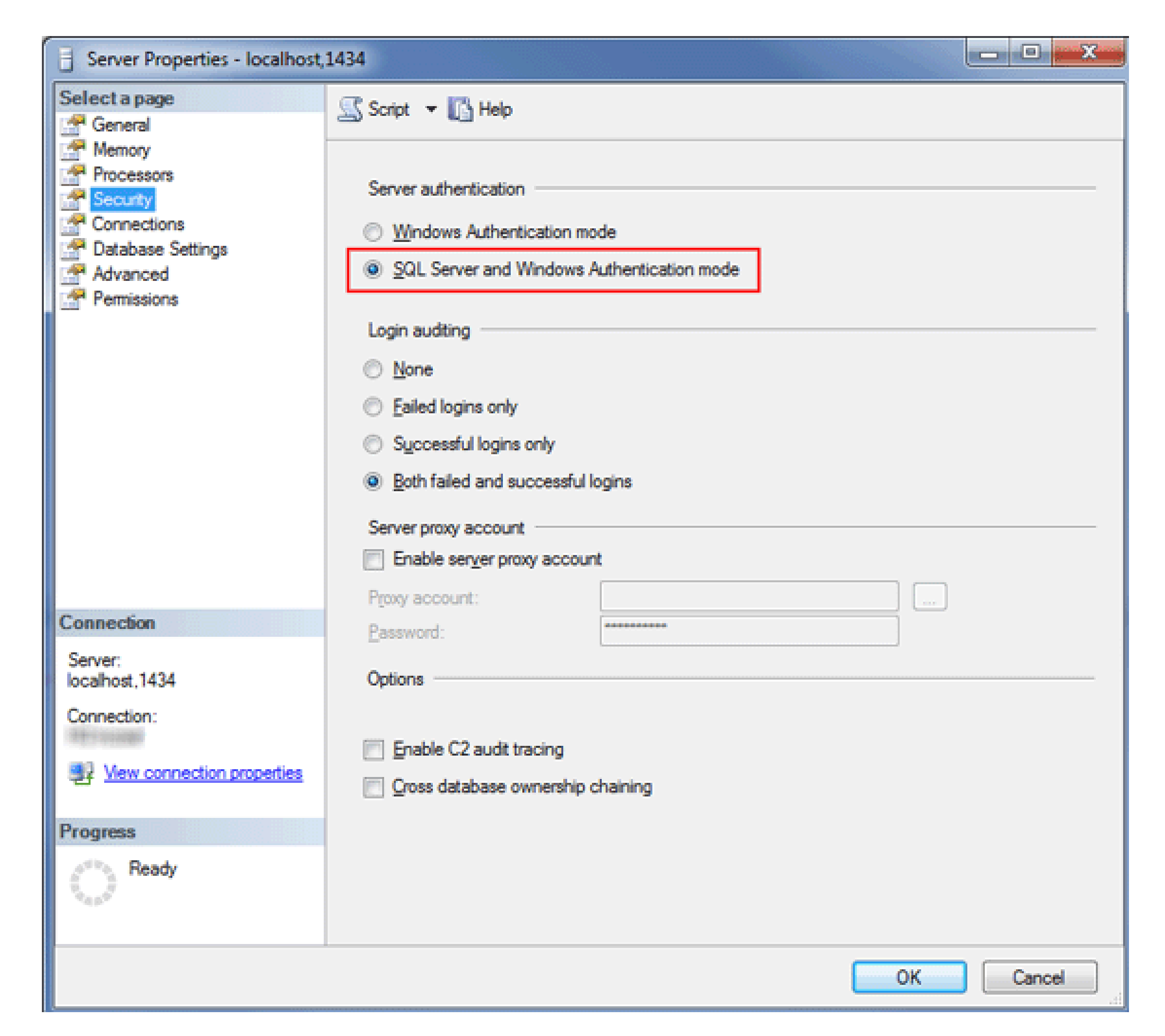
13. Klicken Sie im Wiederherstellungs-Assistenten auf die Seite **Optionen**. Wählen Sie bei Bedarf die Option **Vorhandene Sicherungen überschreiben** aus und stellen Sie sicher, dass die Wiederherstellungsorte für die Datenbank (`.mdf`) und für das Log (`.ldf`) korrekt sind. Wenn Sie die Standardwerte unverändert übernehmen, werden die Pfade von Ihrer SQL Server-Quellinstanz verwendet. Sie sollten diese Werte daher überprüfen.

   - Falls Sie nicht sicher sind, wo die DB-Dateien auf der SQL Server-Zielinstanz liegen, klicken Sie mit der rechten Maustaste auf eine vorhandene Datenbank, wählen Sie **Eigenschaften** aus und klicken Sie auf die Registerkarte **Dateien**. Sie finden den Speicherort der Datenbank in der Spalte **Pfad** der gezeigten Tabelle.



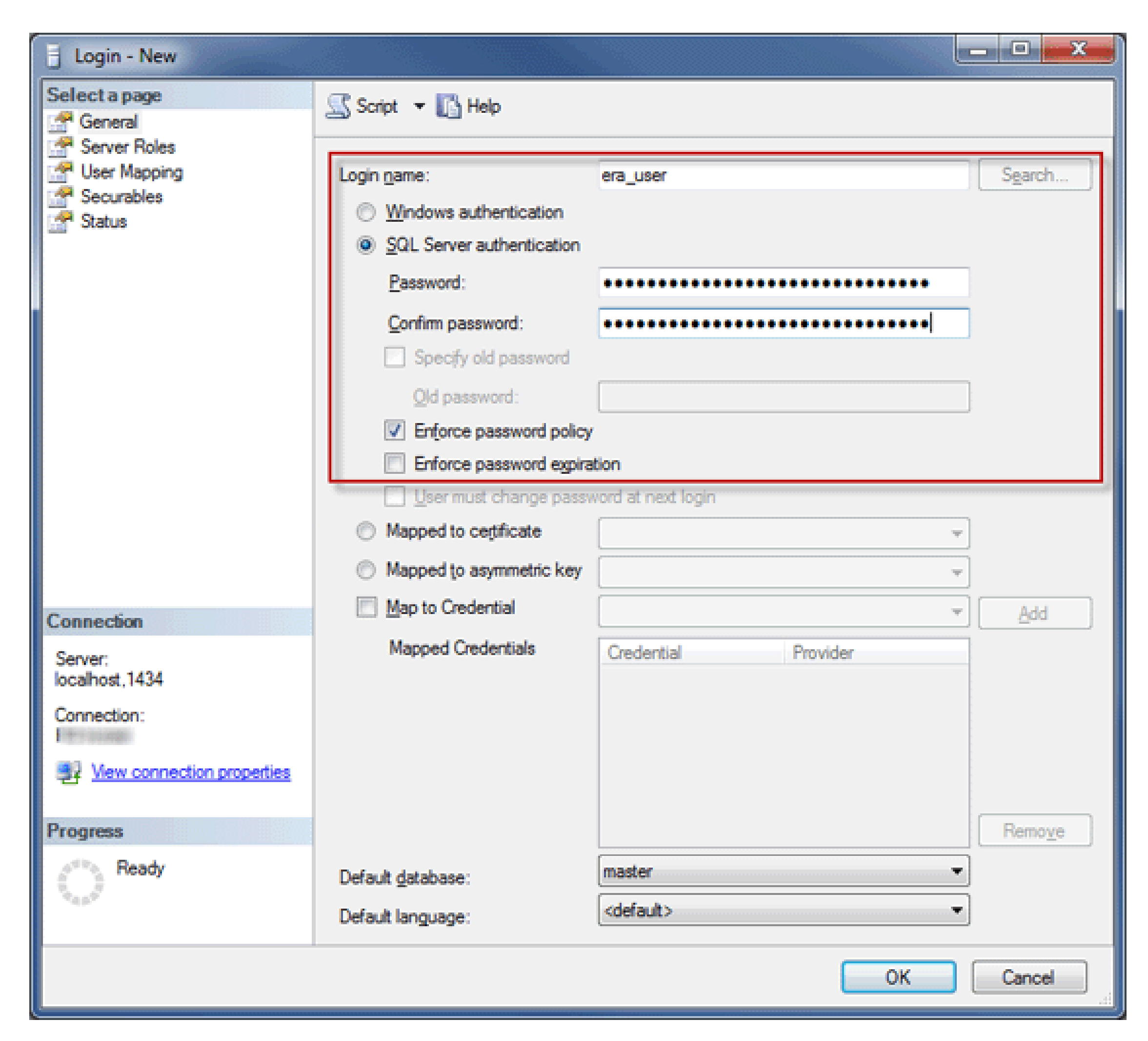
14.Klicken Sie im Wiederherstellung-Assistenten auf **OK**.

15.Stellen Sie sicher, dass im neuen Datenbankserver die **SQL Server-Authentifizierung aktiviert** ist. Klicken Sie mit der rechten Maustaste auf den Server und klicken Sie anschließend auf **Eigenschaften**. Navigieren Sie zu **Sicherheit** und vergewissern Sie sich, dass der SQL Server- und Windows-Authentifizierungsmodus ausgewählt ist.

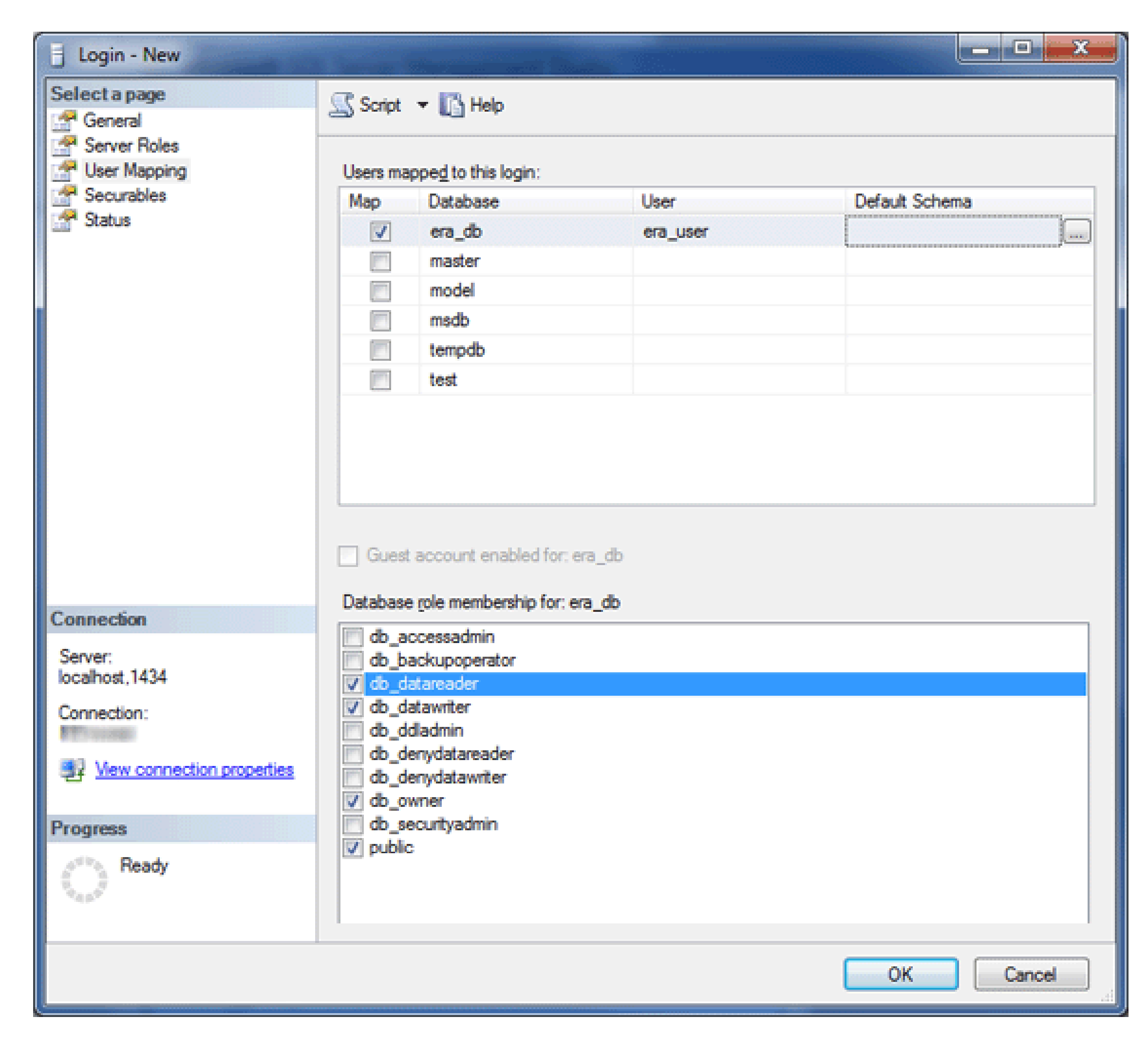


16. **Erstellen Sie eine neue SQL Server-Anmeldung** (für ERA Server/Proxy) auf der SQL Server-Zielinstanz mit **SQL Server-Authentifizierung** und ordnen Sie die Anmeldung zu einem Benutzer in der wiederhergestellten Datenbank zu.

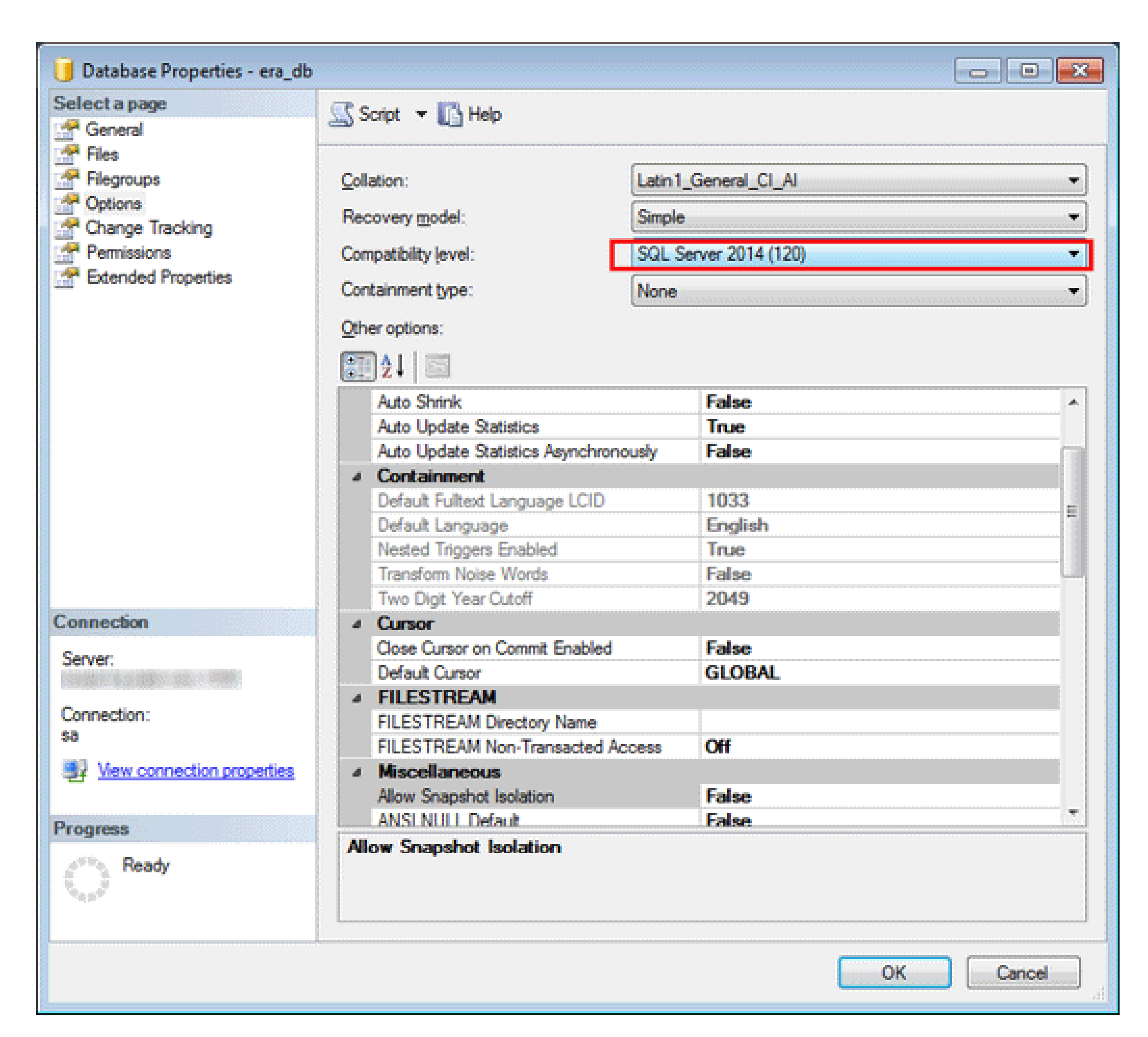
- Deaktivieren Sie unbedingt die Option Kennwortablauf!
- Empfohlene Zeichen für Benutzernamen:
  - ASCII-Kleinbuchstaben, Ziffern und Unterstrich "_"
- Empfohlene Zeichen für Passwörter:
  - AUSSCHLIESSLICH ASCII-Zeichen, inklusive ASCII-Groß- und Kleinbuchstaben, Ziffern, Leerzeichen, Sonderzeichen
- Verwenden Sie keine nicht-ASCII-Zeichen wie z. B. die geschweiften Klammern {} oder @
- Nichtbeachtung der obigen Zeichenempfehlungen kann zu Verbindungsproblemen in der Datenbank führen, falls Sie die Sonderzeichen in den späteren Schritten bei der Modifikation der Datenbankverbindungszeichenfolgen nicht maskieren. Dieses Dokument enthält keine Regeln für die Maskierung von Zeichen.



17. Ordnen Sie die Anmeldung zu einem Benutzer in der Zieldatenbank zu. Vergewissern Sie sich in der Registerkarte Benutzerzuordnungen, dass der Datenbankbenutzer die folgenden Rollen hat: **db_datareader**, **db_datawriter**, **db_owner**.



18.Ändern Sie den **Kompatibilitätsgrad** der wiederhergestellten Datenbank auf die neueste Version, um die aktuellsten Datenbankserver-Features nutzen zu können. Klicken Sie mit der rechten Maustaste auf die neue Datenbank und öffnen Sie deren **Eigenschaften**.



HINWEIS: SQL Server Management Studio kann keine neueren Kompatibilitätsgrade als die der verwendeten Version festlegen. Beispiel: In SQL Server Management Studio 2008 kann der Kompatibilitätsgrad SQL Server 2014 nicht festgelegt werden.

19. **Suchen Sie die Datei** `startupconfiguration.ini` auf dem Computer, auf dem ERA Server/Proxy installiert ist.

   - Windows Vista und neuere Versionen:
     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration \startupconfiguration.ini
   - Ältere Windows-Versionen:
     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData \Configuration\startupconfiguration.ini
   - Linux:
     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

20. **Ändern** Sie die Datenbankverbindungszeichenfolge in ERA Server/Proxy startupconfiguration.ini

   - Tragen Sie Adresse und Port des neuen Datenbankservers ein.
   - Tragen Sie den ERA-Benutzernamen und das ERA-Passwort in die Verbindungszeichenfolge ein.
     - Das Endergebnis sollte wie folgt aussehen:

```
DatabaseType=MSSQLOdbc
DatabaseConnectionString=Driver=SQL Server;Server=localhost,1433;Uid=era_benutzer1;Pwd={GeheimesPassw
```

21. **Starten Sie** den ERA Server/Proxy und vergewissern Sie sich, dass der ERA Server/Proxy-Dienst korrekt ausgeführt wird.

3.2.3.2 Migrationsprozess für MySQL Server

- **Voraussetzungen:**
  - SQL Server-Quell- und Zielinstanzen müssen installiert sein. Diese Instanzen können sich auf unterschiedlichen Computern befinden.
  - Die MySQL-Werkzeuge (mysqldump und mysql-Client) müssen auf mindestens einem der Computer installiert sein.

- **Hilfreiche Links:**

http://dev.mysql.com/doc/refman/5.6/en/copying-databases.html

http://dev.mysql.com/doc/refman/5.6/en/mysqldump.html

http://dev.mysql.com/doc/refman/5.6/en/mysql.html

- Nehmen Sie in den folgenden Befehlen, Konfigurationsdateien und SQL-Anweisungen immer die folgenden Ersetzungen vor:
  - **SRCHOST** mit der Adresse des Quelldatenbankservers
  - **SRCROOTLOGIN** mit der root-Benutzeranmeldung für den MySQL-Quellserver
  - **SRCERADBNAME** mit dem Namen der zu sichernden ERA-Quelldatenbank
  - **BACKUPFILE** mit dem Pfad der Datei, in der die Sicherung gespeichert werden soll
  - **TARGETHOST** mit der Adresse des Zieldatenbankservers
  - **TARGETROOTLOGIN** mit der root-Benutzeranmeldung für den MySQL-Zielserver
  - **TARGETERADBNAME** mit dem Namen der ERA-Zieldatenbank (nach der Migration)
  - **TARGETERALOGIN** mit dem Anmeldenamen für den neuen ERA-Datenbankbenutzer auf dem MySQL-Zielserver
  - **TARGETERAPASSWD** mit dem Passwort des neuen ERA-Datenbankbenutzers auf dem MySQL-Zielserver

Es ist nicht erforderlich, die folgenden SQL-Anweisungen in der Befehlszeile auszuführen. Falls kein GUI-Werkzeug verfügbar ist, können Sie eine Anwendung Ihrer Wahl verwenden.

1. **Beenden** Sie den ERA Server- bzw. ERA Proxy-Dienst.
2. **Erstellen** Sie eine vollständige Datenbanksicherung der ERA-Quelldatenbank (die zu migrierende Datenbank):
```
mysqldump --host SRCHOST --disable-keys --extended-insert -u SRCROOTLOGIN -p SRCERADBNAME > BACKUPFILE
```
3. **Bereiten** Sie eine leere Datenbank auf dem MySQL-Zielserver vor:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE DATABASE TARGETERADBNAME /*!40100 DEFAUL
```

HINWEIS: Verwenden Sie Apostroph ' anstelle von Anführungszeichen " auf Linux-Systemen.

4. **Stellen** Sie die Datenbank auf dem MySQL-Zielserver in die zuvor vorbereitete leere Datenbank her:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETERADBNAME < BACKUPFILE
```
5. **Erstellen** Sie einen ERA-Datenbankbenutzer auf dem MySQL-Zielserver:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=CREATE USER TARGETERALOGIN@'%' IDENTIFIED BY 'T
```

Empfohlene Zeichen für **TARGETERALOGIN**:
- ASCII-Kleinbuchstaben, Ziffern und Unterstrich "_"

Empfohlene Zeichen für **TARGETERAPASSWD**:
- AUSSCHLIESSLICH ASCII-Zeichen, inklusive ASCII-Groß- und Kleinbuchstaben, Ziffern, Leerzeichen und Sonderzeichen
- Verwenden Sie keine nicht-ASCII-Zeichen wie z. B. die geschweiften Klammern {} oder @

Nichtbeachtung der obigen Zeichenempfehlungen kann zu Verbindungsproblemen in der Datenbank führen, falls Sie die Sonderzeichen in den späteren Schritten bei der Modifikation der Datenbankverbindungszeichenfolgen nicht maskieren. Dieses Dokument enthält keine Regeln für die Maskierung von Zeichen**.**

6. **Erteilen** Sie dem ERA-Datenbankbenutzer au dem MySQL-Zielserver die benötigten Zugriffsrechte:
```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--execute=GRANT ALL ON TARGETERADBNAME.* TO TARGETERALOGIN
```

HINWEIS: Verwenden Sie Apostroph ' anstelle von Anführungszeichen " auf Linux-Systemen.

7. **Suchen Sie die Datei** `startupconfiguration.ini` auf dem Computer, auf dem ERA Server/Proxy installiert ist.

   - Windows Vista und neuere Versionen:
     % PROGRAMDATA %\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration \startupconfiguration.ini

   - Ältere Windows-Versionen:
     % ALLUSERSPROFILE %\ Application Data\ESET\RemoteAdministrator\Server\EraServerApplicationData \Configuration\startupconfiguration.ini

   - Linux:
     /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

8. **Ändern** Sie die Datenbankverbindungszeichenfolge in ERA Server/Proxy `startupconfiguration.ini`
   - Tragen Sie Adresse und Port des neuen Datenbankservers ein
   - Geben Sie Benutzername und Passwort ein

     - Das Endergebnis sollte wie folgt aussehen:
```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port=3306;User=TARGETERAI
```

9. **Starten Sie** den ERA Server/Proxy und vergewissern Sie sich, dass der ERA Server/Proxy-Dienst korrekt ausgeführt wird.

3.3 ISO-Abbild

Das ESET Remote Administrator-Installationsprogramm kann unter anderem als ISO-Abbilddatei (Kategorie All-in-One-Installationspakete) heruntergeladen werden. Das ISO-Abbild enthält Folgendes:

- ERA-Installationspaket
- Getrennte Installationsprogramme für jede Komponente

Das ISO-Abbild ist besonders nützlich, wenn sie alle ESET Remote Administrator-Installationsprogramme an einem Ort aufbewahren möchten. Wenn Sie über ein ISO-Abbild verfügen, müssen Sie die Installationsprogramme nicht für jede Installation von der ESET-Website herunterladen. Das ISO-Abbild ist auch hilfreich, wenn Sie ESET Remote Administrator auf einer virtuellen Maschine installieren möchten.

3.4 Virtuelle Appliance

Der ERA-Server kann in einer VMware- oder Microsoft Hyper-V-Umgebung bereitgestellt werden. Dier virtuelle ERA-Appliance wird als OVA -Datei (Open Virtualization Appliance) bereitgestellt. Die OVA-Datei ist eine Vorlage, die ein funktionsfähiges CentOS 6.5-Betriebssystem enthält. Mit der entsprechenden Vorlage können Sie entweder ERA-Server, ERA-Proxy oder ERA MDM bereitstellen. Befolgen Sie bei der Bereitstellung einer OVF-Vorlage in VMware die Anweisungen des Einrichtungsassistenten zum Festlegen des Passworts für das ERA-Administratorkonto und konfigurieren Sie vor der Bereitstellung die virtuelle Maschine. Nach der Bereitstellung der Appliance stellt die virtuelle Maschine eine vollständige Umgebung mit einsatzbereitem ESET Remote Administrator dar.

Virtuelle ERA-Appliances sind vom virtuellen Hardwaretyp „vmx-07“ und werden daher von den folgenden VMware Hypervisors unterstützt:

- ESXi 5.0 und höher
- Workstation 6.5 und höher

Sie können auch VMware Player oder Oracle VirtualBox auf einem Desktop-Betriebssystem verwenden und die virtuelle Appliance mit dieser Konfiguration bereitstellen. Auf diese Weise können Sie ESET Remote Administrator auf Hardware mit Nicht-Server-Betriebssystem und ohne Unternehmens-ESXi ausführen. Dieser Abschnitt gilt nur für die Datei `ERA_Server.ova`.

Bereitstellen einer OVF-Vorlage in einem vSphere-Client

1. Verbinden Sie sich über den vSphere-Client mit dem vCenter-Server (verbinden Sie sich nicht direkt mit dem ESXi-Server).
2. Klicken Sie in der oberen Menüleiste auf **Datei** und wählen Sie **OVF-Vorlage bereitstellen** aus.
3. Klicken Sie auf **Durchsuchen**, Navigieren Sie zu der OVA-Datei , die Sie von der ESET-Website heruntergeladen haben und klicken Sie auf Öffnen. Je nach geplanter Bereitstellung verwenden Sie entweder die Datei `ERA_Server.ova`, `ERA_Proxy.ova` oder `ERA_MDM.ova`.
4. Klicken Sie im Fenster mit den OVF-Vorlagendetails auf **Weiter**.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
6. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen. Geben Sie hierbei die folgenden Informationen für den virtuellen Client an:
   – Name und Speicherort
   – Host/Cluster
   – Ressourcen-Pool
   – Speicher
   – Datenträgerformat
   – Netzwerkzuordnung
6. Geben Sie auf der Seite **„Eigenschaften“** einen **Hostnamen** (Hostname des ERA-Servers oder des ERA-Proxy) und ein **Passwort** an. Das Passwort wird in allen ERA-Komponenten (ERA-Datenbank, ERA-Server und ERA-Web-Konsole) und für den Zugriff auf den virtuelle ERA-Computer (CentOS) verwendet und ist daher sehr wichtig.

7. Die Eingabe in die übrigen Felder ist optional. Sie können die Details der **Windows-Domäne** angeben. Dies ist nützlich für die Synchronisierung der statischen Gruppen. Sie können auch **Netzwerkeigenschaften** festlegen.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

Source
OVF Template Details
End User License Agreement
Name and Location
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete

Application

Hostname
The fully qualified hostname for this VM (e.g.: era.domain.com). Leave blank to try to reverse lookup the IP address.

Password
VM, database and server (webconsole) password.
Enter password **********
Confirm password **********

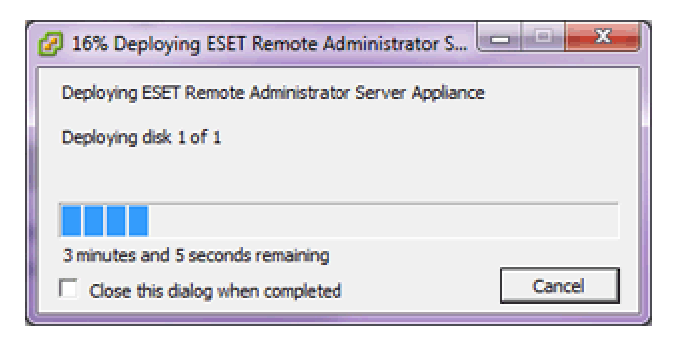
Locale
The locale used for pre-defined objects created during installation.
en-US

Windows Domain
The domain for this server (e.g.: domain.com). Leave blank if no domain synchronization and authorization will be performed.
franto

Windows Domain Controller
The domain controller for this server (e.g.: dc.domain.com). If domain controller hostname is not recognized by default DNS server, please set this domain controller's IP address as DNS server for this VM. Leave blank if no domain actions will be performed.

Help | < Back | Next > | Cancel

8. Klicken Sie auf **Weiter**, überprüfen Sie die Bereitstellungszusammenfassung und klicken Sie auf **Fertig stellen**. Der Vorgang erstellt automatisch einen virtuellen Computer mit den ausgewählten Einstellungen. Nachdem die VM erstellt ist, können Sie sie aktivieren.



9. Wenn Sie nach der Bereitstellung von ERA die VMware-Konsole öffnen, werden die folgenden Informationen und die URL der ERA Web-Konsole im Format „https://[IP-Adresse]:8443“ angezeigt. Geben Sie die URL in Ihrem Webbrowser ein, um sich bei der ERA-Web-Konsole anzumelden (verwenden Sie das in Schritt 6 festgelegte Passwort).

```
ESET Remote Administrator Server Appliance
(C) 2014 ESET, spol. s r.o. - All rights reserved

Server version: 6.1.355.0
Agent version: 6.1.355.0
Rogue Detection Sensor version: 1.0.668.0

ERA Server hostname: era.local
ERA Server IP address: 10.1.119.54
ERA Server port: see configuration (default is 2222)

To open ERA web console please use the following links:
https://era.local:8443
https://10.1.119.54:8443



<ENTER> Enter management mode
```

HINWEIS: Es wird dringend empfohlen, die vCenter-Rollen und -Berechtigungen so zu konfigurieren, dass die VMware-Benutzer keinen Zugriff auf die virtuelle ERA-Maschine haben. So wird vermieden, dass Benutzer die virtuelle ERA-Maschine manipulieren. ERA-Benutzer benötigen keinen Zugriff auf die VM. Den eigentlichen Zugriff auf ESET Remote Administrator können Sie im Bereich Zugriffsrechte in der ERA Web-Konsole verwalten.

3.4.1 VMware Player

Bereitstellen einer OVF-Vorlage in VMware Player

Verwenden Sie unbedingt die neueste Version von VMware Player.

1. Wählen Sie **Datei** > **Virtuelle Maschine öffnen** aus.

2. Navigieren Sie zu der OVA-Datei (`ERA_Server.ova`), die Sie von der ESET-Website heruntergeladen haben. Klicken Sie auf **Öffnen**.

3. Geben Sie einen Namen und einen lokalen Speicherpfad für die neue virtuelle Maschine ein und klicken Sie auf **Importieren.**

4. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), falls Sie dieser zustimmen.

5. Nachdem die Appliance erstellt wurde, können Sie diese aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

First time appliance configuration was not possible because OVF
environment was not found. If you are deploying on non ESXi
platform then manual configuration is needed:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
   nano ovf.xml
4. Restart appliance by typing:
   shutdown -r now

Default generated OVF configuration will configure this appliance
as server with password [eraadmin] with all other options turned off
and with DHCP network settings. To apply this configuration, just
restart appliance from root terminal.


<ENTER> Enter management mode
```

6. Bearbeiten Sie die Konfigurationsdatei `ovf.xml` und geben Sie Ihre Datenbankverbindungsdetails usw. ein. Folgen Sie dazu den Anweisungen auf dem Bildschirm.

3.4.2 Oracle VirtualBox

Bereitstellen einer OVA-Datei in VirtualBox

Verwenden Sie unbedingt die neueste Version von VirtualBox.

1. Klicken Sie auf **Datei** und anschließend auf **Appliance importieren...**
2. Klicken Sie auf **Durchsuchen** und navigieren Sie zu der OVA-Datei (`ERA_Server.ova`), die Sie von der ESET-Website heruntergeladen haben und klicken Sie auf Öffnen. Klicken Sie auf **Weiter**.
3. Überprüfen Sie Ihre Appliance-Einstellungen und klicken Sie auf **Importieren**.
4. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA), falls Sie dieser zustimmen.
5. Nachdem die Appliance erstellt wurde, können Sie diese aktivieren. Die folgenden Informationen werden angezeigt:

```
ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

First time appliance configuration was not possible because OVF
environment was not found. If you are deploying on non ESXi
platform then manual configuration is needed:
1. Enter management mode with password [eraadmin].
2. Exit console to root terminal.
3. Edit and save OVF configuration XML for server by typing:
   nano ovf.xml
4. Restart appliance by typing:
   shutdown -r now

Default generated OVF configuration will configure this appliance
as server with password [eraadmin] with all other options turned off
and with DHCP network settings. To apply this configuration, just
restart appliance from root terminal.


<ENTER> Enter management mode
```

6. Bearbeiten Sie die Konfigurationsdatei `ovf.xml` und geben Sie Ihre Datenbankverbindungsdetails usw. ein. Folgen Sie dazu den Anweisungen auf dem Bildschirm.

3.4.3 Microsoft Hyper-V

Bereitstellen einer OVA-Datei in Microsoft Hyper-V

1. Extrahieren Sie die (von der ESET-Website heruntergeladenen) Dateien aus der Datei der virtuellen Appliance (`ERA_Server.ova`) mit einem Hilfsprogramm wie Tar oder 7-Zip. Daraufhin sehen Sie eine Anzahl extrahierter Dateien, inklusive der `.vmdk`- Datei (z. B. `ERA_Server-disk1.vmdk`extrahieren).

2. Laden Sie Microsoft Virtual Machine Converter 3.0 http://www.microsoft.com/en-us/download/details.aspx?id=42497 herunter und installieren Sie die Software.

3. Stellen Sie sicher, dass Windows PowerShell 3.0 (oder neuer) auf Ihrem System verfügbar ist, insbesondere unter Windows 7. Führen Sie dazu die folgenden Schritte aus:

   a. Öffnen Sie die Windows-Eingabeaufforderung (**cmd.exe**).
   b. Geben Sie `powershell`in der Befehlszeile ein und drücken Sie die Eingabetaste.
   c. Geben Sie in der PowerShell den Befehl `$PSVersionTable` ein und drücken Sie die **Eingabetaste**.
   d. Falls **PSVersion 3.0** (oder neuer) angezeigt wird, fahren Sie mit Schritt 5 fort. Laden Sie andernfalls Windows Management Framework 3.0 http://www.microsoft.com/en-us/download/details.aspx?id=34595 herunter und installieren Sie die Software.
   e. Wiederholen Sie die Schritte a-c, um sicherzustellen, dass PowerShell 3.0 oder neuer installiert ist, und fahren Sie anschließend mit Schritt 5 fort.

4. Öffnen Sie PowerShell und führen Sie die Befehle in den folgenden Schritten aus.

5. Führen Sie den "Import module"-Befehl aus:
```
import-Module 'C:\Program Files\Microsoft Virtual Machine Converter\MvmcCmdlet.psd1'
```

6. Überprüfen Sie die importierten Module mit dem folgenden Befehl, um sicherzustellen, dass der Importvorgang erfolgreich war:
```
get-command -Module mvmccmdlet
```

7. Konvertieren Sie das `.vmdk`-Laufwerk, dass Sie in Schritt 1 extrahiert haben. (`ERA_Server-disk1.vmdk`, falls Sie ERA-Server bereitstellen):

a. Unter Windows 7 müssen Sie das **VHD-Format** verwenden:

```
ConvertTo-MvmcVirtualHardDisk -SourceLiteralPath <path>\ERA_Server-disk1.vmdk -
DestinationLiteralPath <output-dir> -VhdType DynamicHardDisk -VhdFormat Vhd
```

b. Unter Windows 8 und höher können Sie das **VHDX-Format** verwenden:

```
ConvertTo-MvmcVirtualHardDisk -SourceLiteralPath <path>\ERA_Server-disk1.vmdk -
DestinationLiteralPath <output-dir> -VhdType DynamicHardDisk -VhdFormat Vhdx
```

8. Verbinden Sie sich mit Hyper-V.

9. Erstellen Sie einen neuen virtuellen Computer (Generation 1) mit mindestens 4 Prozessorkernen und 4 GB Arbeitsspeicher. Dieser virtuelle Computer wird das in Schritt 7 konvertierte Laufwerk verwenden.

3.5 Failover-Cluster - Windows

Zur Installation von ESET Remote Administrator in einer Failover-Cluster-Umgebung sind im Wesentlichen folgende Schritte erforderlich:

1. Erstellen Sie ein Failover-Cluster. Der Cluster sollte über einen freigegebenen Datenträger, eine IP-Adresse und einen Clusternamen verfügen.
   a. Anweisungen zum Erstellen eines Failover-Clusters unter Windows Server 2012
   b. Anweisungen zum Erstellen eines Failover-Clusters unter Windows Server 2008
2. Installieren Sie ERA-Server und den ERA-Agenten auf dem aktiven Knoten. Wählen Sie den freigegebenen Datenträger als Datenspeicher für die Anwendung.
3. Ändern Sie den aktiven Knoten und wiederholen Sie Schritt 2.
4. Erstellen Sie im Clusterkonfigurations-Manager 2 Clusterdienste: ERA-Agent und ERA-Server.
5. Legen Sie die geeigneten Abhängigkeiten fest: Die Dienste sollten gestartet werden, nachdem die Ressourcen aus Schritt 1 initialisiert sind. Außerdem sollte der ERA-Agent vom ERA-Server abhängig sein.
6. Datenbank und Web-Server werden in einem Cluster nicht unterstützt.

HINWEIS: Es ist nicht möglich, den ERA-Server mit dem ERA-Installationsprogramm in einem Failover-Cluster zu installieren. Um ESET Remote Administrator in einem Failover-Cluster zu installieren, führen Sie eine Komponenteninstallation aus.

3.6 Failover-Cluster - Linux

Die folgenden Informationen gelten für die Installation und Konfiguration von ESET Remote Administrator in einem Red Hat-Hochverfügbarkeitscluster.

- Linux-Clusterunterstützung
- Voraussetzungen
- Umfang
- Installationsschritte

Linux-Clusterunterstützung

Server und ERA-Proxy können in **Red Hat Linux 6**-Clustern und höheren Versionen installiert werden. Failover-Cluster werden im aktiven/passiven Modus nur mit dem Clustermanager **rgmanager** unterstützt.

Voraussetzungen

- Ein aktiver/passiver Cluster muss installiert und konfiguriert sein. Es kann jeweils nur ein Knoten auf einmal aktiv sein. Die anderen Knoten müssen im Bereitschaftsmodus sein. Lastenausgleich wird nicht unterstützt.

- Freigegebener Speicher- Es werden iSCSI SAN, NFS und weitere Lösungen unterstützt (beliebige Technologien, die block- oder dateibasierten Zugriff auf den freigegebenen Speicher bieten und die freigegebenen Geräte dem Betriebssystem als lokal angeschlossene Geräte anzeigen). Der freigegebene Speicher muss von jedem aktiven Knoten im Cluster zugreifbar sein und das freigegebene Dateisystem muss richtig initialisiert sein (beispielsweise mit dem EXT3- oder EXT4-Dateisystem).

- Für die Systemverwaltung sind folgende Hochverfügbarkeits-Add-ons erforderlich:
    - rgmanager
    - Conga

- **rgmanager** ist der übliche Red Hat-Hochverfügbarkeits-Clusterstapel. Er ist eine obligatorische Komponente.

- Die **Conga**-Benutzeroberfläche ist optional. Der Failover-Cluster kann ohne Conga verwaltet werden. Für eine optimale Leistung empfehlen wir jedoch, Conga zu installieren. In diesem Handbuch gehen wir davon aus, dass es installiert ist.

- muss korrekt konfiguriert sein, um eine Datenbeschädigung zu vermeiden. Wenn die Umgrenzung noch nicht konfiguriert ist, muss der Clusteradministrator sie konfigurieren.

Wenn noch kein Cluster ausgeführt wird, steht Ihnen folgendes Handbuch zur Verfügung, um ein Hochverfügbarkeits-Failover-Cluster (aktiv/passiv) unter Red Hat einzurichten: Red Hat Enterprise Linux 6 - Clusterverwaltung.

Umfang

ESET Remote Administrator-Komponenten, die in einem **Red Hat Linux**-Hochverfügbarkeits-Cluster installiert werden können:

- ERA-Server mit ERA-Agent
- ERA-Proxy mit ERA-Agent

HINWEIS: Der ERA-Agent muss installiert werden, da andernfalls der ERA-Clusterdienst nicht ausgeführt wird.

HINWEIS: Die Installation der ERA-Datenbank oder der ERA-Web-Konsole in einem Cluster wird nicht unterstützt.

Das folgende Installationsbeispiel beschreibt ein Cluster mit 2 Knoten. Sie können ESET Remote Administrator jedoch in einem Cluster mit mehreren Knoten installieren und dieses Beispiel nur als Referenz verwenden. Die Clusterknoten in diesem Beispiel sind „node1“ und „node2“.

Installationsschritte

1. Installieren Sie den ERA-Server oder den ERA-Proxy und dann den ERA-Agenten auf „node1“. Wenn Sie während der Installation des ERA-Agenten den Befehl `--hostname=` verwenden, können Sie `localhost` angeben (geben Sie nicht die IP-Adresse oder den eigentlichen Hostnamen des betroffenen Knotens an). Alternativ können Sie die externe IP-Adresse oder den Hostnamen der Clusterschnittstelle angeben.

- Achtung: Der Hostname im Server- bzw. Proxyzertifikat muss die externe IP (bzw. den externen Hostnamen) der Clusterschnittstelle enthalten (nicht die lokale IP bzw. den lokalen Hostnamen des Knotens).
- Wenn Sie während der Installation des ERA-Agenten den Befehl "--hostname=" verwenden, haben Sie die folgenden Optionen:
    - Sie können die externe IP-Adresse oder den Hostnamen der Clusterschnittstelle angeben.
    - Alternativ können Sie localhost angeben (anstelle von IP-Adresse oder Hostname des jeweiligen Knotens). In diesem Fall muss der Hostname im ERA Server- bzw. ERA Proxy-Zertifikat zusätzlich den Eintrag localhost enthalten.

2. Stoppen und deaktivieren Sie die Linux-Dienste des ERA-Agenten und des ERA-Servers bzw. ERA-Proxy. Verwenden Sie dazu folgende Befehle:

```
chkconfig eraagent off
chkconfig eraserver off
service eraagent stop
service eraserver stop
```

3. Hängen Sie den freigegebenen Speicher in „node1“ ein. In diesem Beispiel wird der freigegebene Speicher unter **/usr/share/erag2cluster** eingehängt.

4. Erstellen Sie unter **/usr/share/erag2cluster** die folgenden Verzeichnisse:

   /usr/share/erag2cluster/etc/opt
   /usr/share/erag2cluster/opt
   /usr/share/erag2cluster/var/log
   /usr/share/erag2cluster/var/opt

5. Verschieben Sie die folgenden Verzeichnisse rekursiv an die angegebenen Zielsorte (Ursprung > Ziel):

Verschieben Sie den Ordner:	Nach:
/etc/opt/eset	/usr/share/erag2cluster/etc/opt/
/opt/eset	/usr/share/erag2cluster/opt/
/var/log/eset	/usr/share/erag2cluster/var/log/
/var/opt/eset	/usr/share/erag2cluster/var/opt/

6. Erstellen Sie symbolische Verknüpfungen:

ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset

7. Heben Sie das Einhängen des freigegebenen Speichers unter „node1“ auf und hängen Sie den freigegebenen Speicher auf „node2“ im gleichen Verzeichnis wie zuvor auf „node1“ (**/usr/share/erag2cluster**) ein.

8. Erstellen Sie auf „node2“ die folgenden symbolischen Verknüpfungen:

ln -s /usr/share/erag2cluster/etc/opt/eset /etc/opt/eset
ln -s /usr/share/erag2cluster/opt/eset /opt/eset
ln -s /usr/share/erag2cluster/var/log/eset /var/log/eset
ln -s /usr/share/erag2cluster/var/opt/eset /var/opt/eset

9. Kopieren Sie das Skript `eracluster_server` (`eracluster_proxy`) nach **/usr/share/cluster**.

   Die Skripts `eracluster_server` (`eracluster_proxy`) befinden sich im Setupverzeichnis von ERA-Server bzw. ERA-Proxy.

Die nächsten Schritte werden in der Conga-Clusterverwaltungsoberfläche ausgeführt:

10. Erstellen Sie eine Dienstgruppe, zum Beispiel „EraService“.

Der ESET Remote Administrator-Clusterdienst benötigt drei Ressourcen: IP-Adresse, Dateisystem und Skript.

11. Erstellen Sie die erforderlichen Dienstressourcen.

   Fügen Sie eine IP-Adresse, ein Dateisystem und Skriptressourcen hinzu.
   Die Dateisystemressource muss auf den freigegebenen Speicher zeigen.
   Der Einhängepunkt der Dateisystemressource muss auf **/usr/share/erag2cluster** festgelegt werden.
   Der Parameter „Vollständiger Pfad zur Skriptdatei“ der Skriptressource muss auf **/usr/share/cluster/eracluster_server** (bzw. **/usr/share/cluster/eracluster_proxy**) festgelegt werden

12. Fügen Sie die oben genannten Ressourcen zur Gruppe „EraService“ hinzu.

3.7 Komponenteninstallation unter Windows

In den meisten Installationsszenarien müssen Sie verschiedene ESET Remote Administrator-Komponenten auf verschiedenen Computern installieren, beispielsweise um Unterschiede in der Netzwerkarchitektur zu berücksichtigen oder Leistungsanforderungen zu erfüllen. Für diese Art der Installation sind Installationspakte für einzelne Komponenten verfügbar.

Kernkomponenten

- ERA-Server
- ERA-Web-Konsole
- ERA-Agent (muss auf Clientcomputern installiert sein, optional auf dem ERA-Server)

Optionale Komponenten

- ERA-Proxy
- RD Sensor
- Connector für Mobilgeräte
- Apache-HTTP-Proxy

Informationen zum Aktualisieren von ESET Remote Administrator auf die neueste Version (6.x) finden Sie in unserem Knowledgebase-Artikel.

3.7.1 Serverinstallation – Windows

Befolgen Sie diese Schritte, um die ERA-Serverkomponente unter Windows zu installieren:

1. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind.

2. Führen Sie das Installationsprogramm für den ERA-Server aus und akzeptieren Sie die EULA, wenn Sie ihr zustimmen.

HINWEIS: Wenn Sie den ERA-Server in einem Failover-Cluster installieren, aktivieren Sie das Kontrollkästchen neben **Dies ist eine Clusterinstallation**. Andernfalls lassen Sie dieses Kontrollkästchen deaktiviert.

3. Geben Sie bei einer Installation in einem Failover-Cluster den **Benutzerdefinierten Anwendungsdatenpfad** ein, der auf den freigegebenen Speicher des Clusters zeigt. Die Daten müssen an einem einzigen Speicherort gespeichert sein, auf den alle Knoten im Cluster zugreifen können.

4. Geben Sie einen gültigen ERA-Lizenzschlüssel ein oder wählen Sie **Später aktivieren** aus.

5. Wählen Sie ein **Dienstbenutzerkonto** aus. Mit diesem Konto wird der ESET Remote Administrator-Serverdienst ausgeführt. Folgende Optionen stehen zur Verfügung:

   - Netzwerkdienstkonto
   - Bestimmter Benutzer: DOMÄNE/BENUTZERNAME

4. Stellen Sie eine Verbindung zu einer Datenbank her. Hier werden alle Daten gespeichert (Passwort für die ERA Web-Konsole, Logs der Clientcomputer usw.):

   - **Datenbank**: MySQL Server/MS SQL Server/MS SQL Server mit Windows-Authentifizierung
   - **ODBC-Treiber**: MySQL ODBC 5.1-Treiber/MySQL ODBC 5.2 Unicode-Treiber/MySQL ODBC 5.3 Unicode-Treiber/ SQL Server/SQL Server Native Client 10.0/ODBC-Treiber 11 für SQL Server
   - **Datenbankname**: Sie können den vordefinierten Namen lassen oder ihn bei Bedarf ändern.
   - **Hostname**: Hostname oder IP-Adresse des Datenbankservers
   - **Port:** für die Verbindung zum Datenbankserver
   - **Benutzername**/**Passwort** des Datenbankadministratorkontos

HINWEIS: Der ERA-Server speichert große Datenblöcke in der Datenbank. Daher muss MySQL zur Annahme großer Pakete konfiguriert sein, damit ERA ordnungsgemäß funktioniert. Ausführliche Informationen zu dieser Konfiguration finden Sie in unseren FAQ.

In diesem Schritt wird die Verbindung zur Datenbank überprüft. Wenn die Verbindung erfolgreich ist, können Sie zum nächsten Schritt fortfahren.

5. Wählen Sie einen Benutzer für ESET Remote Administrator aus, der zum Zugriff auf die Datenbank berechtigt ist. Sie können einen vorhandenen Benutzer angeben oder einen neuen Benutzer erstellen lassen.

6. Geben Sie ein Passwort für den Zugriff auf die **Web-Konsole** ein.

7. ESET Remote Administrator verwendet Zertifikate für die Client-Server-Kommunikation. Wählen Sie entweder Ihre eigenen Zertifikate aus oder lassen Sie vom **Server** neue Zertifikate erstellen.

8. Geben Sie das Passwort für die **Zertifizierungsstelle** ein. Merken Sie sich das Passwort gut.

9. Ein neuer Zertifikatserver wird erstellt. Wählen Sie erneut ein Passwort aus.

10. Wählen Sie im nächsten Schritt ein Passwort für das **Agenten**-Zertifikat aus.

Während der Einrichtung kann ein erster Task zur Synchronisierung der statischen Gruppen ausgeführt werden. Wählen Sie die Methode aus (**Nicht synchronisieren**, **Mit Windows-Netzwerk synchronisieren**, **Mit Active Directory synchronisieren**) und klicken Sie auf **Weiter**.

Bestätigen oder ändern Sie den Installationsordner für den Server und klicken Sie auf **Weiter**.

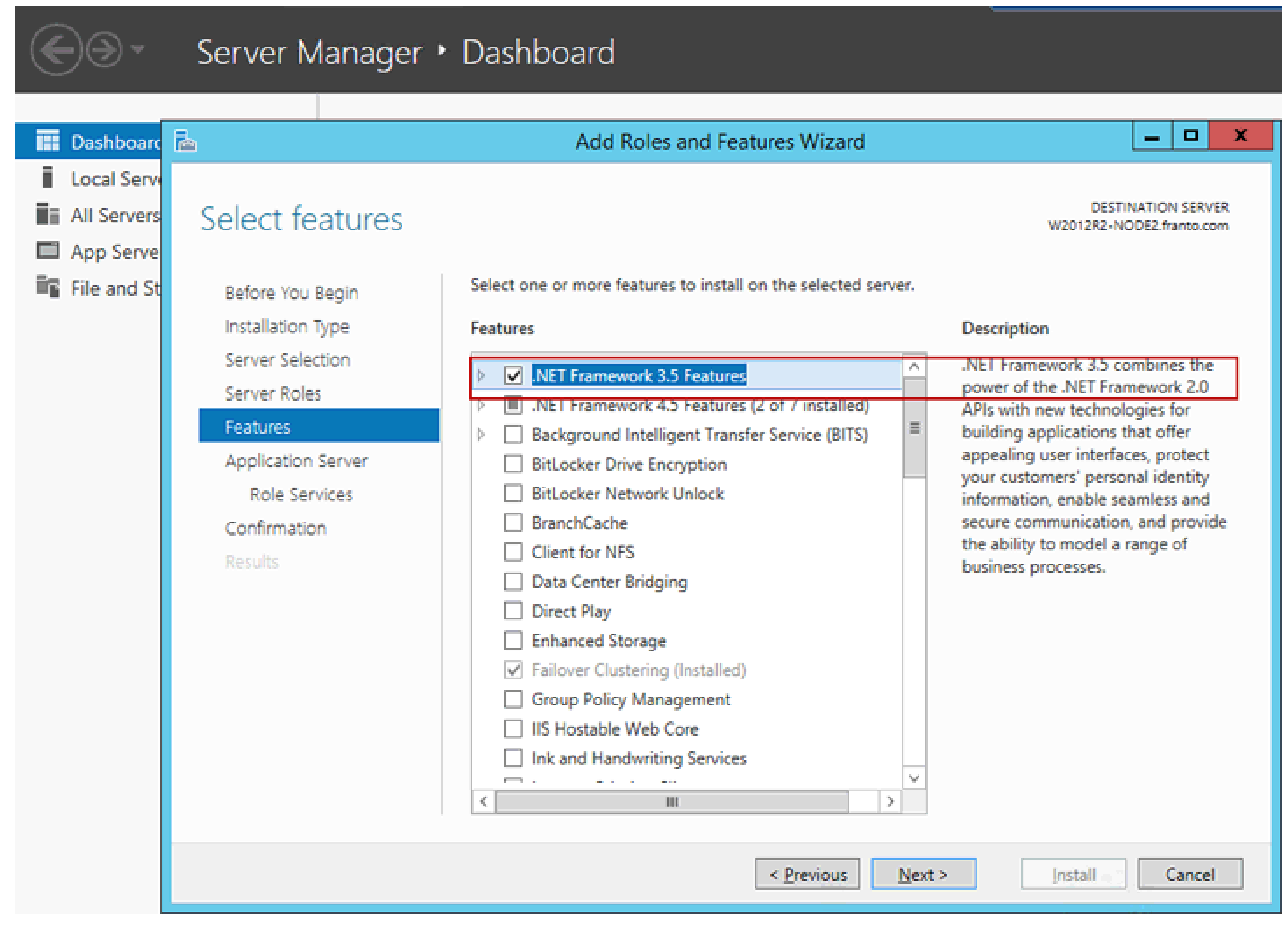
Klicken Sie auf **Installieren**, um den Server zu installieren.

HINWEIS: Nachdem Abschluss der Installation des ERA-Servers können Sie den ERA-Agenten auf dem gleichen Computer installieren (optional). Auf diese Weise können Sie den Server auf dieselbe Weise verwalten wie einen Clientcomputer.

3.7.1.1 Servervoraussetzungen – Windows

Für die Installation des ERA-Servers unter Windows müssen folgende Voraussetzungen erfüllt sein:

- Sie benötigen eine gültige Lizenz.
- Die erforderlichen Ports müssen geöffnet und verfügbar sein. Eine vollständige Liste der Ports finden Sie hier.
- Datenbankserver (Microsoft SQL Server oder MySQL) installiert und aktiv, siehe Datenbank-Anforderungen für Details. Falls Sie keinen vorhandenen Datenbankserver haben, sollten Sie die Schritte unter SQL Server-Konfiguration ausführen, um den SQL Server für den Einsatz mit ESET Remote Administrator zu konfigurieren.
- Die Java Runtime Environment (JRE) muss installiert sein (erhältlich unter http://java.com/en/download/). Verwenden Sie immer die jeweils aktuellste Java-Version.
- Microsoft .NET Framework 3.5 muss installiert sein. Wenn Sie Windows Server 2008 oder 2012 verwenden, können Sie es über den **Assistenten zum Hinzufügen von Rollen und Features** (Abbildung unten) installieren. Wenn Sie Windows Server 2003 verwenden, können Sie .NET 3.5 hier herunterladen: http://www.microsoft.com/en-us/download/details.aspx?id=21



HINWEIS: Wenn Sie Microsoft SQL Server Express während der Installation von ESET Remote Administrator installieren, können Sie es nicht auf einem Domänencontroller installieren. Dies ist üblicherweise der Fall, wenn Sie Microsoft SBS. verwenden. Wenn Sie Microsoft SBS verwenden, empfiehlt es sich, ESET Remote Administrator auf einem anderen Server zu installieren oder während der Installation nicht die SQL Server Express-Komponente auszuwählen (Sie müssen dann zum Ausführen der ERA-Datenbank SQL Server oder MySQL verwenden). Anweisungen zur Installation des ERA-Servers auf einem Domänencontroller finden Sie in unserem Knowledgebase-Artikel.

HINWEIS: Der ERA-Server speichert große Datenblöcke in der Datenbank. Daher muss MySQL zur Annahme großer Pakete konfiguriert sein, damit ERA ordnungsgemäß funktioniert. Anweisungen zum Vornehmen dieser Änderung finden Sie in den FAQ.

3.7.2 Microsoft SQL Server - Windows

Eine der Voraussetzungen für die Installation des ERA-Servers ist ein installierter und für den Einsatz mit ESET Remote Administrator konfigurierter Microsoft SQL Server. Die folgenden Voraussetzungen müssen erfüllt sein:

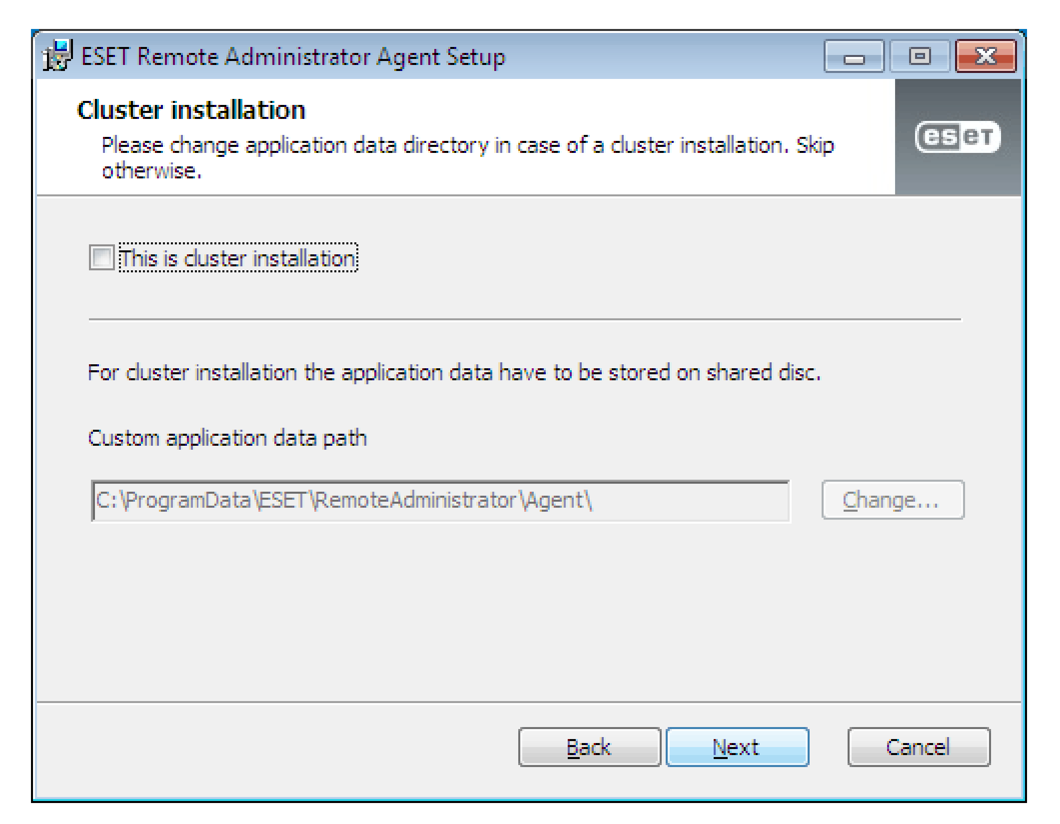
- Installieren Sie Microsoft SQL Server 2008 R2 oder eine neuere Version. Alternativ können Sie Microsoft SQL Server 2008 R2 Express oder eine neuere Version installieren. Wählen Sie bei der Installation den **Gemischten Modus** für die Authentifizierung aus.
- Falls Sie Microsoft SQL Server bereits installiert haben, setzen Sie die Authentifizierung auf **Gemischter Modus (SQL Server-Authentifizierung und Windows-Authentifizierung)**. Führen Sie dazu die Anweisungen in diesem KnowledgeBase-Artikel aus.
- Erlauben Sie TCP/IP-Verbindungen zum SQL Server. Führen Sie dazu die Anweisungen in diesem KnowledgeBase-Artikel aus Teil **II. Erlauben Sie TCP/IP-Verbindungen zum SQL Server** aus.

3.7.3 Agenten-Installation – Windows

Befolgen Sie diese Schritte, um die ERA-Agentenkomponente unter Windows zu installieren:

1. Führen Sie das Installationsprogramm für den ERA-Agenten aus und akzeptieren Sie die EULA, wenn Sie ihr zustimmen.

HINWEIS: Wenn Sie den ERA-Agenten in einem Failover-Cluster installieren, aktivieren Sie das Kontrollkästchen neben **Dies ist eine Clusterinstallation**. Andernfalls lassen Sie dieses Kontrollkästchen deaktiviert.



2. Geben Sie bei einer Installation in einem Failover-Cluster den **Benutzerdefinierten Anwendungsdatenpfad** ein, der auf den freigegebenen Speicher des Clusters zeigt. Die Daten müssen an einem einzigen Speicherort gespeichert sein, auf den alle Knoten im Cluster zugreifen können.
3. Geben Sie den **Server-Host** (Name oder IP-Adresse des ERA-Servers) und den **Serverport** (standardmäßig 2222; ersetzen Sie diesen Wert durch einen benutzerdefinierten Port, falls Sie einen anderen Port verwenden) ein.

Wählen Sie eine der folgenden Installationsoptionen und führen Sie die Schritte aus, die in den entsprechenden Abschnitten beschrieben sind:

- **Servergestützte Installation** - Hierzu müssen Sie die Anmeldedaten des Administrators der ERA-Webkonsole eingeben (das Installationsprogramm lädt automatisch die erforderlichen Zertifikate herunter).
- **Offline-Installation** - Hierzu müssen Sie ein **Agentenzertifikat** angeben, das Sie aus ESET Remote Administrator exportieren können. Alternativ können Sie ein benutzerdefiniertes Zertifikat verwenden.

Servergestützte Installation:

4. Geben Sie den **Server-Host** (Name oder IP-Adresse des ERA-Servers) und den **Web-Konsolen-Port** ein (lassen Sie den standardmäßigen Port 2223 unverändert, sofern Sie keinen benutzerdefinierten Port verwenden). Geben Sie außerdem die Anmeldedaten des Administrators der Web-Konsole ein: **Benutzername**/**Passwort**.

5. Klicken Sie auf „Ja“, wenn Sie gefragt werden, ob Sie das Zertifikat akzeptieren möchten.

6. Wählen Sie **Computer nicht erstellen** oder **Benutzerdefinierte statische Gruppe auswählen** aus. Wenn Sie auf **Benutzerdefinierte statische Gruppe auswählen** klicken, können Sie aus einer Liste vorhandener statischer Gruppen in ERA eine Auswahl treffen. Der Computer wird der ausgewählten Gruppe hinzugefügt.

7. Geben Sie einen Zielordner für den ERA-Agenten an (wir empfehlen, den standardmäßigen Speicherort beizubehalten), klicken Sie auf **Weiter**und dann auf **Installieren**.

Offline-Installation:

4. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort des Peerzertifikats (es handelt sich dabei um das Agentenzertifikat, dass Sie aus ERA exportiert haben). Lassen Sie das Textfeld **Zertifikatspasswort** leer, da für dieses Zertifikat kein Passwort erforderlich ist. Sie müssen keine **Zertifizierungsstelle** suchen. Lassen Sie dieses Feld leer.

HINWEIS: Wenn Sie ein benutzerdefiniertes Zertifikat mit ERA verwenden (anstelle des standardmäßigen, das automatisch während der Installation von ESET Remote Administrator generiert wurde), geben Sie dies entsprechend an.

5. Klicken Sie auf **Weiter**, um die Installation im standardmäßigen Ordner auszuführen, oder klicken Sie auf **Ändern**, um einen anderen Ordner auszuwählen. Wir empfehlen, den standardmäßigen Speicherort beizubehalten.

3.7.4 Installation der Web-Konsole – Windows

Führen Sie diese Schritte aus, um die ERA Web-Konsole unter Windows zu installieren:

1. Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind:

   - Java - Verwenden Sie immer die aktuellste Java-Version (Obwohl die ERA Web-Konsole mindestens Java Version 7 benötigt, empfehlen wir dringend die Verwendung der aktuellsten offiziellen Java-Version).
   - Apache Tomcat (Version 6 oder höher).
   - Datei der Web-Konsole (*era.war*) auf der lokalen Festplatte gespeichert.

2. Kopieren Sie die Datei *era.war* in den Tomcat-Ordner für Webanwendungen (auf den meisten Betriebssystemen: *C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\).*

3. Starten Sie den *Apache Tomcat*-Dienst neu.

4. Öffnen Sie https://localhost/era/ in einem Browser auf dem Localhost. Ein Anmeldebildschirm wird angezeigt.

3.7.4.1 Unterstützte Webbrowser

Webbrowser	Version
Mozilla Firefox	20+
Internet Explorer	10+
Chrome	23+
Safari	6+
Opera	12+

3.7.5 Proxyinstallation – Windows

Befolgen Sie diese Schritte, um den ERA-Proxyserver unter Windows zu installieren:

1. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind.

HINWEIS: Wenn Sie den ERA-Proxyserver in einem Failover-Cluster installieren, aktivieren Sie das Kontrollkästchen **Dies ist eine Clusterinstallation**. Andernfalls lassen Sie dieses Kontrollkästchen deaktiviert.

2. Geben Sie bei einer Installation in einem Failover-Cluster den **Benutzerdefinierten Anwendungsdatenpfad** ein, der auf den freigegebenen Speicher des Clusters zeigt. Die Daten müssen an einem einzigen Speicherort gespeichert sein, auf den alle Knoten im Cluster zugreifen können.

3. Wählen Sie das Konto eines Dienstbenutzers aus. Mit diesem Konto wird der ESET Remote Administrator-Serverdienst ausgeführt. Folgende Optionen stehen zur Verfügung:

   a. Netzwerkdienstkonto
   b. Benutzerdefiniertes Konto: DOMÄNE/BENUTZERNAME

4. Stellen Sie eine Verbindung zu einer Datenbank her. Hier werden alle Daten gespeichert, vom Passwort für die ERA Web-Konsole zu den Logs der Clientcomputer.

   a. Datenbank: MySQL/MS SQL
   b. ODBC-Treiber: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 ANSI/ DriverSQL Server
   c. Hostname des Datenbankservers
   d. Port, der für die Verbindung zum Server verwendet wird
   e. Datenbankname
   f. Anmeldename/Passwort des Datenbankadministrators
   g. Anmeldename/Passwort des ERA-Datenbankbenutzers

In diesem Schritt wird die Verbindung zur Datenbank überprüft. Wenn die Verbindung erfolgreich ist, können Sie zum **nächsten** Schritt fortfahren. Wenn die Verbindung nicht hergestellt werden kann, wird eine Fehlermeldung angezeigt.

4. Wählen Sie einen Kommunikationsport für den Proxyserver aus. Standardmäßig wird Port 2222 verwendet.

5. Konfigurieren Sie die Proxyverbindung zu ESET Remote Administrator. Geben Sie einen Enter a **Server-Hostnamen** (Hostname/IP-Adresse des Servers) und den **Serverport** (2222) an.

6. Wählen Sie ein Peerzertifikat und ein Passwort für das Zertifikat aus. Fügen Sie optional eine Zertifizierungsstelle hinzu. Dies ist nur für nicht signierte Zertifikate erforderlich.

7. Wählen Sie einen Ordner aus, in dem der **Proxy** installiert wird, oder lassen Sie den vordefinierten Ordner ausgewählt.

8. Klicken Sie auf **Installieren**. Der **Proxy** wird auf dem Computer installiert.

HINWEIS: Die servergestützte Installation wird bei der Installation von ERA-Proxy nicht unterstützt.

3.7.5.1 Proxyservervoraussetzungen – Windows

Zur Installation des ERA-Proxyservers unter Windows müssen folgende Voraussetzungen erfüllt sein:

- **Der ERA-Server** und die **ERA Web-Konsole** sind installiert (auf einem Servercomputer).
- Ein **Proxyzertifikat** ist erstellt und wurde zum lokalen Laufwerk heruntergeladen.
- Eine **Zertifizierungsstelle** ist auf dem lokalen Laufwerk vorbereitet.
- Eine gültige Lizenz ist vorhanden.
- Ein Datenbankserver ist bereits installiert und konfiguriert.
- Ein ODBC-Treiber zur Verbindung mit dem Datenbankserver (MySQL / MS SQL) ist auf dem Computer installiert.
- Der Agent muss auf einem lokalen Computer installiert sein, damit alle Programmfunktionen vollständig unterstützt werden.

3.7.6 Rogue Detection Sensor-Installation – Windows

Befolgen Sie diese Schritte, um RD Sensor unter Windows zu installieren:

1. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind.
2. Doppelklicken Sie auf die RD Sensor-Installationsdatei, um die Installation zu beginnen.
3. Wählen sie den Speicherort zum Installieren von RD Sensor aus und klicken Sie auf **Weiter** > **Installieren**.

3.7.6.1 Rogue Detection Sensor-Voraussetzungen – Windows

Zur Installation der RD Sensor-Komponente unter Windows müssen folgende Voraussetzungen erfüllt sein:

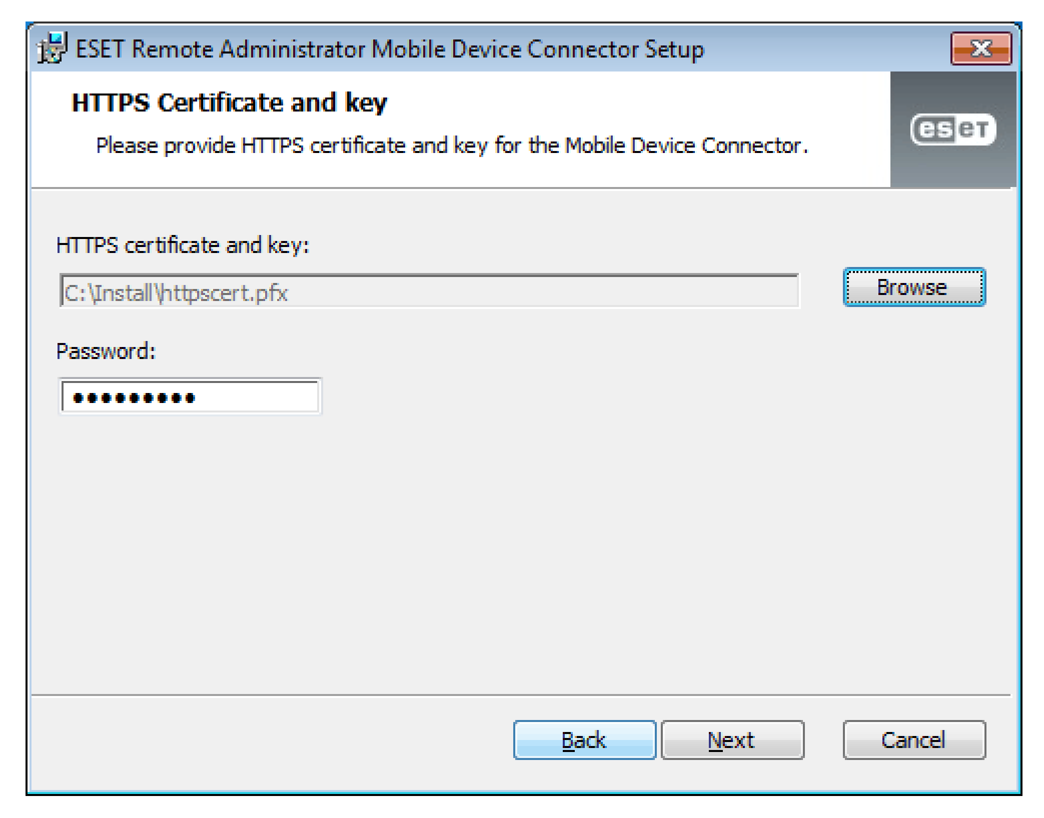
- WinPcap - verwenden Sie die neueste WinPcap-Version (mindestens 4.1.0)
- Das Netzwerk muss korrekt konfiguriert sein (entsprechende Ports geöffnet, eingehende Kommunikation nicht durch Firewall gesperrt, usw.)
- Der ERA-Server muss erreichbar sein
- Der ERA-Agent muss auf einem lokalen Computer installiert sein, um alle Programmfunktionen vollständig zu unterstützen
- Die Log-Datei des Rogue Detection Sensor befindet sich unter folgendem Pfad: *C:\ProgramData\ESET\Rouge Detection Sensor\Logs\trace.log*

3.7.7 Installation des Connectors für Mobilgeräte - Windows

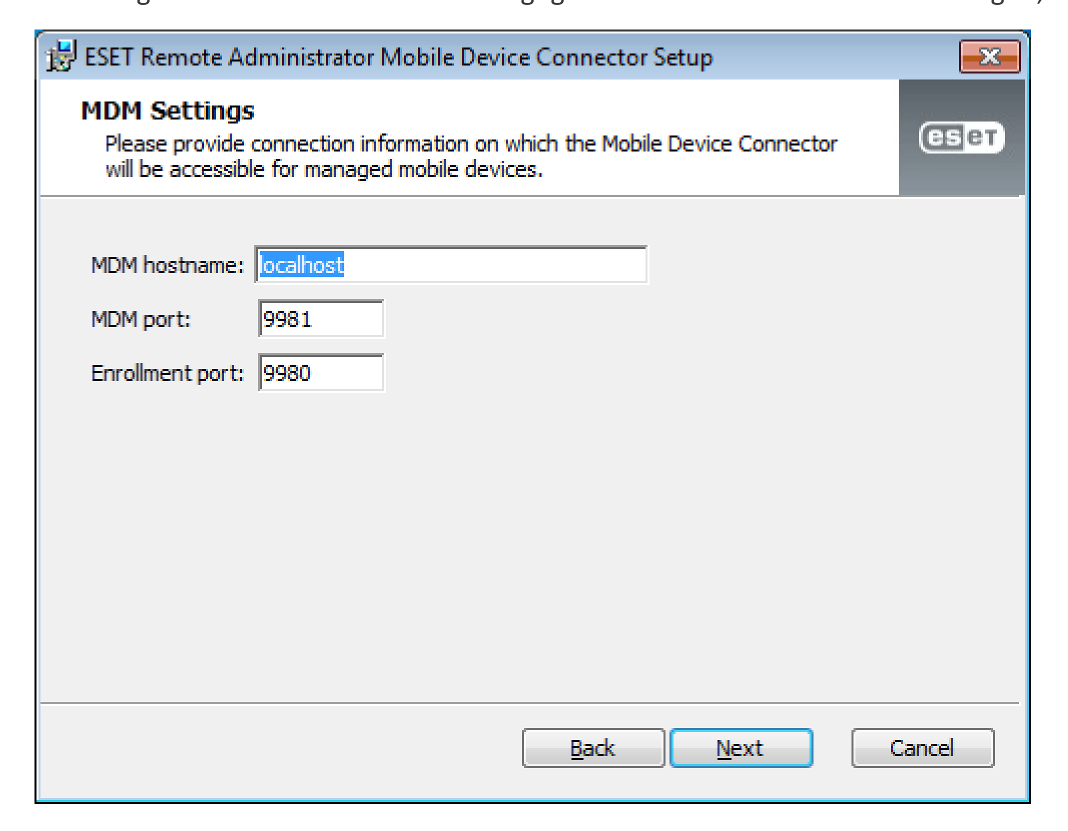
Sie können den Connector für Mobilgeräte auf einem anderen Server installieren, als der Server, auf dem der ERA-Server ausgeführt wird. Dies ist beispielsweise sinnvoll, wenn über das Internet auf den Connector für Mobilgeräte zugegriffen werden soll, um die Mobilgeräte der Benutzer jederzeit und unabhängig von ihrem Standort verwalten zu können.

Führen Sie die nachfolgenden Schritte aus, um den Connector für Mobilgeräte unter Windows zu installieren:

1. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind.
2. Führen Sie das Installationsprogramm für den Connector für Mobilgeräte aus und akzeptieren Sie die EULA, sofern Sie mit ihr zustimmen.
3. Klicken Sie auf **Durchsuchen**, navigieren Sie zum Speicherort des SSL-Zertifikats für die Kommunikation über HTTPS und geben Sie das Passwort für dieses Zertifikat ein:



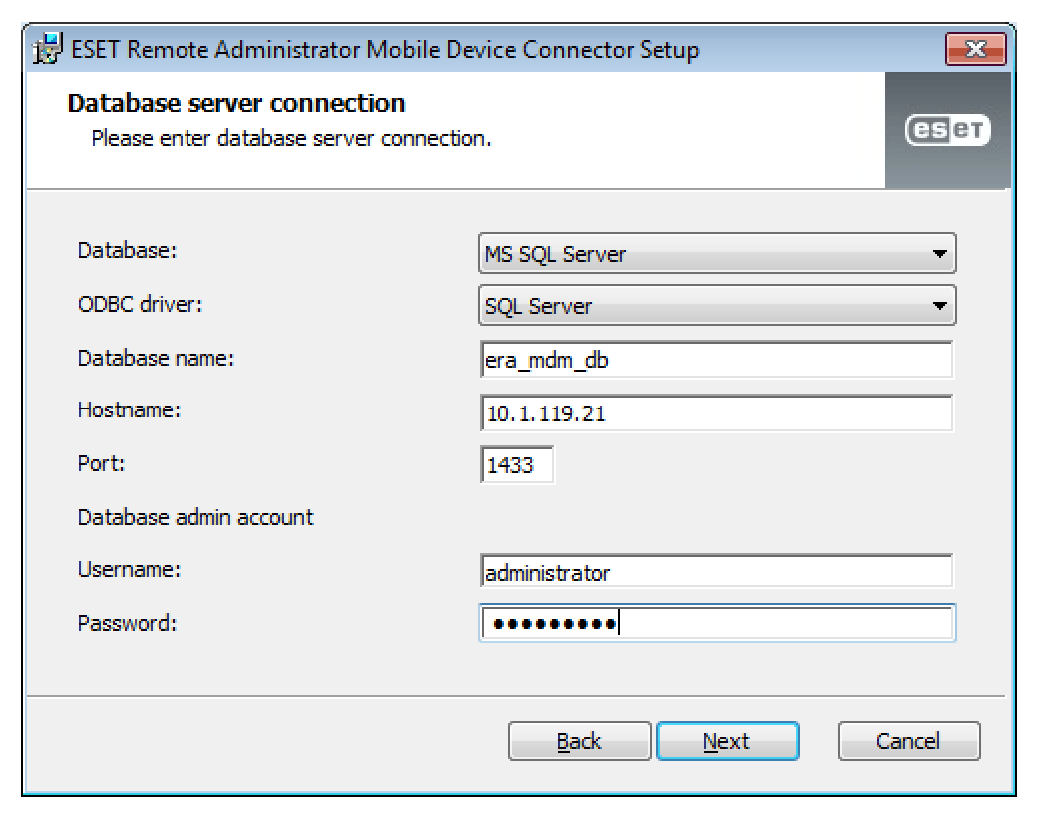
4. Es empfiehlt sich, den standardmäßigen Hostnamen und die standardmäßigen Ports (9981 und 9980) zu verwenden. Bei Bedarf können Sie jedoch auch eigene Ports angeben. Vergewissern Sie sich, dass die Geräte über diese beiden Ports eine Verbindung zum Server herstellen können, auf dem Sie den Connector für Mobilgeräte installieren. Ändern Sie gegebenenfalls die Firewalleinstellungen, um dies zu ermöglichen.



5. Das Installationsprogramm muss eine neue Datenbank erstellen, die vom Connector für Mobilgeräte verwendet wird. Geben Sie hierfür folgende Verbindungsdetails ein:

   - **Datenbank**: MySQL Server/MS SQL Server/MS SQL Server mit Windows-Authentifizierung
   - **ODBC-Treiber**: MySQL ODBC 5.1-Treiber/MySQL ODBC 5.2 Unicode-Treiber/MySQL ODBC 5.3 Unicode-Treiber/ SQL Server/SQL Server Native Client 10.0/ODBC-Treiber 11 für SQL Server
   - **Datenbankname**: Sie können den vordefinierten Namen lassen oder ihn bei Bedarf ändern.
   - **Hostname**: Hostname oder IP-Adresse des Datenbankservers
   - **Port:** für die Verbindung zum Datenbankserver
   - **Benutzername**/**Passwort** des Datenbankadministratorkontos

HINWEIS: Es empfiehlt sich, den gleichen Datenbankserver wie für die ERA-Datenbank zu verwenden. Bei Bedarf können Sie jedoch auch einen anderen Datenbankserver verwenden. Klicken Sie auf die Schaltfläche „Weiter“. Das Installationsprogramm für den Connector für Mobilgeräte erstellt eine Datenbank.



6. Geben Sie den Benutzer für die neu erstellte Datenbank des Connectors für Mobilgeräte an. Sie können einen **Neuen Benutzer erstellen** oder den **Bestehenden Benutzer verwenden**. Geben Sie das Passwort für den Datenbankbenutzer ein.

7. Geben Sie den **Server-Host** (Name oder IP-Adresse des ERA-Servers) und den **Serverport** (standardmäßig 2222; ersetzen Sie diesen Wert durch einen benutzerdefinierten Port, falls Sie einen anderen Port verwenden) ein.

Nun stehen Ihnen zum Fortsetzen der Installation zwei Möglichkeiten zur Verfügung:

- **Servergestützte Installation** - Hierzu müssen Sie die Anmeldedaten des Administrators der ERA-Webkonsole eingeben (das Installationsprogramm lädt automatisch die erforderlichen Zertifikate herunter).
- **Offline-Installation** - Hierzu müssen Sie ein **Agentenzertifikat** angeben, das Sie aus ESET Remote Administrator exportieren können. Alternativ können Sie ein benutzerdefiniertes Zertifikat verwenden.

Die folgenden Schritte gelten für die Option **Servergestützte Installation**:

8. Geben Sie den **Server-Host** (Name oder IP-Adresse des ERA-Servers) und den **Web-Konsolen-Port** ein (lassen Sie den standardmäßigen Port 2223 unverändert, sofern Sie keinen benutzerdefinierten Port verwenden). Geben Sie außerdem die Anmeldedaten des Administrators der Web-Konsole ein: **Benutzername**/**Passwort**.

9. Wenn die Frage **Zertifikat annehmen?** angezeigt wird, klicken Sie auf **Ja**.

10. Geben Sie einen Zielordner für den Connector für Mobilgeräte an (wir empfehlen, den standardmäßigen Speicherort beizubehalten), klicken Sie auf **Weiter**und dann auf **Installieren**.

Folgende Schritte sind anwendbar, wenn Sie die **Offline-Installation** wählen:

8. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort des Peerzertifikats (es handelt sich dabei um das Agentenzertifikat, dass Sie aus ERA exportiert haben). Lassen Sie das Textfeld **Zertifikatspasswort** leer, da für dieses Zertifikat kein Passwort erforderlich ist.

HINWEIS: Wenn Sie mit ERA benutzerdefinierte Zertifikate (anstelle der standardmäßigen, automatisch während der Installation von ESET Remote Administrator generierten Zertifikate) verwenden, verwenden Sie die benutzerdefinierten Zertifikate hier entsprechend.

9. Klicken Sie auf **Weiter**, um die Installation im standardmäßigen Ordner auszuführen, oder klicken Sie auf **Ändern ...**, um einen anderen Ordner auszuwählen. Wir empfehlen, den standardmäßigen Speicherort beizubehalten.

Überprüfen Sie nach dem Abschluss der Installation, ob der Connector für Mobilgeräte richtig ausgeführt wird. Öffnen Sie hierzu in einem Webbrowser die Adresse 'https://*ihr-mdm-hostname*:*registrierungs-port* (zum Beispiel 'https://eramdm:9980'). Wenn die Installation erfolgreich war, wird folgende Meldung angezeigt:

eset REMOTE ADMINISTRATOR

MDM Server up and running!

Sie können diese URL außerdem dazu verwenden, um die Verfügbarkeit des Connectors für Mobilgeräte aus dem Internet zu überprüfen (sofern so konfiguriert), indem Sie beispielsweise mit einem Mobilgeräte auf die URL zugreifen. Wenn Sie die Seite nicht erreichen können, überprüfen Sie die Firewall und die Konfiguration der Netzwerkinfrastruktur.

3.7.7.1 Voraussetzungen für den Connector für Mobilgeräte - Windows

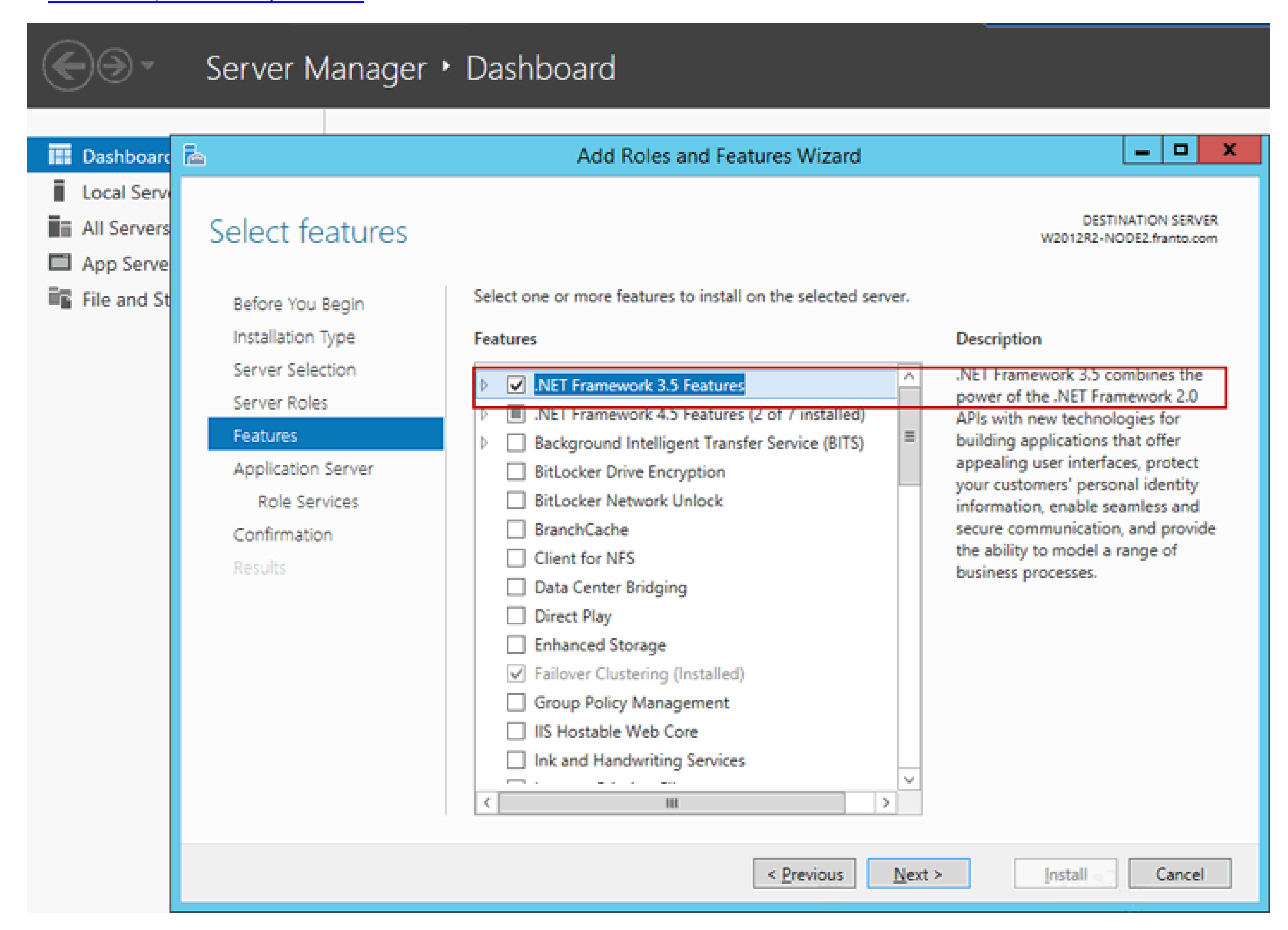
Zur Installation des Connectors für Mobilgeräte unter Windows müssen folgende Voraussetzungen erfüllt sein:

- Die erforderlichen Ports sind geöffnet und verfügbar. Eine vollständige Liste der Ports finden Sie hier.
- Firewall-Einstellungen - falls Sie den Connector für Mobilgeräte auf einem nicht-Server-BS wie z. B. Windows 7 installieren (nur zu Testzwecken), müssen Sie die Kommunikations-Ports öffnen. Erstellen Sie dazu Firewallregeln für:
  C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP Port 9980
  C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP Port 9981
  C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP Port 2222
  C:\Program Files\Apache HTTP Proxy\bin\httpd.exe, TCP Port 3128

  HINWEIS: Die tatsächlichen Pfade zu den .exe-Dateien können je nach Installationsort der ERA-Komponenten auf Ihrem Client-Betriebssystem abweichen.

- Die Java Runtime Environment (JRE) muss installiert sein (erhältlich unter http://java.com/en/download/). Verwenden Sie immer die jeweils aktuellste Java-Version.

- Microsoft .NET Framework 3.5 muss installiert sein. Wenn Sie Windows Server 2008 oder 2012 verwenden, können Sie es über den **Assistenten zum Hinzufügen von Rollen und Features** (Abbildung unten) installieren. Wenn Sie Windows Server 2003 verwenden, können Sie .NET 3.5 hier herunterladen: http://www.microsoft.com/en-us/download/details.aspx?id=21



HINWEIS: Wenn Sie Microsoft SQL Server Express während der Installation von ESET Remote Administrator installieren, können Sie es nicht auf einem Domänencontroller installieren. Dies ist üblicherweise der Fall, wenn Sie Microsoft SBS. verwenden. Wenn Sie Microsoft SBS verwenden, empfiehlt es sich, ESET Remote Administrator auf einem anderen Server zu installieren oder während der Installation nicht die SQL Server Express-Komponente auszuwählen (Sie müssen dann zum Ausführen der ERA-Datenbank SQL Server oder MySQL verwenden).

HINWEIS: Der ERA-Server speichert große Datenblöcke in der Datenbank. Daher muss MySQL zur Annahme großer Pakete konfiguriert sein, damit ERA ordnungsgemäß funktioniert. Anweisungen zum Vornehmen dieser Änderung finden Sie in den FAQ.

WICHTIG: Sie benötigen ein **SSL-Zertifikat** im `.pfx` -Format, um eine sichere Verbindung über HTTPS herstellen zu können. Wir empfehlen, ein von einer Zertifizierungsstelle bereitgestelltes Zertifikat zu verwenden. Selbstsignierte Zertifikate werden nicht empfohlen, da einige Mobilgeräte dem Benutzer nicht die Möglichkeit bieten, selbstsignierte anzunehmen. Bei der Verwendung von Zertifikaten, die von einer Zertifizierungsstelle signiert sind, stellt dies kein Problem dar, weil diese Zertifikate vertrauenswürdig sind und keine Annahme durch den Benutzer erforderlich ist.

WICHTIG: Bei einer Offline-Installation benötigen Sie außerdem ein Peerzertifikat (das **Agentenzertifikat**, das Sie aus ESET Remote Administrator exportiert haben). Alternativ können Sie mit ERA ein benutzerdefiniertes Zertifikat verwenden.

3.7.8 Apache HTTP Proxy-Installation – Windows

Apache HTTP-Proxy ist ein Dienst, der zusammen mit ESET Remote Administrator 6 und neueren Versionen verwendet werden kann, um Updates an Clientcomputer und Installationspakete an den ERA-Agenten zu verteilen. HTTP-Proxy dient einem ähnlichen Zweck wie das beliebte Spiegelserver-Feature in ESET Remote Administrator 5 und früheren Versionen. HTTP-Proxy bietet die folgenden Vorzüge:

- Download neuer Updates für Signaturdatenbanken und Produktkomponenten und deren Verteilung an Clients in Ihrem Netzwerk.
- Zwischenspeicherung von Installationspaketen für ESET-Produkte.
- Minimierung des Internet-Datenverkehrs in Ihrem Netzwerk.

Führen Sie die folgenden Schritte aus, um die Apache HTTP-Proxy-Komponente unter Windows zu installieren:

1. Öffnen Sie ApacheHttp.zip und extrahieren Sie die Dateien nach *C:\Program Files\Apache HTTP Proxy*
2. Öffnen Sie ein Eingabeaufforderungsfenster als Administrator und wechseln Sie in das Verzeichnis *C:\Program Files\Apache HTTP Proxy\bin*
3. Führen Sie den folgenden Befehl aus:

```
httpd.exe -k install -n ApacheHttpProxy
```

4. Öffnen Sie die Datei httpd.conf mit einem Texteditor, beispielsweise Notepad. Fügen Sie am Ende der Datei die folgenden Zeilen hinzu:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

5. Starten Sie den Proxy-Dienst mit dem folgenden Befehl:

```
sc start ApacheHttpProxy
```

6. Im Snap-In services.msc können Sie überprüfen, ob der Apache HTTP-Proxy-Dienst ausgeführt wird (suchen Sie nach „ApacheHttpProxy“). Standardmäßig ist der Dienst so konfiguriert, dass er automatisch gestartet wird.

Führen Sie die folgenden Schritte aus, um einen Benutzernamen und ein Passwort für den Apache HTTP-Proxy zu konfigurieren (empfohlen):

1. Prüfen Sie, ob die folgenden Module in *Apache HTTP Proxy\conf\httpd.conf* vorhanden sind:

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

2. Fügen Sie die folgenden Zeilen zu *Apache HTTP Proxy\conf\httpd.conf* unter `<Proxy *>` hinzu:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

3. Erstellen Sie mit dem Befehl `htpasswd` eine Datei mit dem Namen `password.file` im Ordner *Apache HTTP Proxy \bin* (Sie werden zur Eingabe des Passworts aufgefordert):

```
htpasswd.exe -c ..\password.file username
```

4. Erstellen Sie die Datei `group.file` im Ordner *Apache HTTP Proxy* manuell mit dem folgenden Inhalt:

```
usergroup:username
```

5. Testen Sie die Verbindung zum HTTP Proxy, indem Sie die folgende URL in Ihrem Browser öffnen:

http://localhost:3128/index.html

Verwenden Sie htcacheclean, um den Datenträgercache zu leeren. Dieses Tool kann manuell oder im Daemon-Modus ausgeführt werden. Geben Sie das Limit für die Gesamtgröße des Datenträgercache ein. Der Wert wird standardmäßig in Byte angegeben (oder durch Anfügen von B an die Zahl). Hängen Sie K für Kilobyte oder M für Megabyte an.

Weitere Informationen finden Sie in diesem Knowledgebase-Artikel oder in der Apache-Dokumentation für Authentifizierung und Autorisierung.

3.8 Komponenteninstallation unter Linux

In den meisten Installationsszenarien müssen Sie verschiedene ESET Remote Administrator-Komponenten auf verschiedenen Computern installieren, beispielsweise um Unterschiede in der Netzwerkarchitektur zu berücksichtigen oder Leistungsanforderungen zu erfüllen.

Kernkomponenten

- ERA-Server
- ERA-Web-Konsole
- ERA-Agent

Optionale Komponenten

- ERA-Proxy
- RD Sensor
- Connector für Mobilgeräte
- Apache-HTTP-Proxy

Informationen zum Aktualisieren von ESET Remote Administrator auf die neueste Version (6.x) finden Sie in unserem Knowledgebase-Artikel.

3.8.1 Serverinstallation – Linux

Die Installation der ERA-Serverkomponente unter Linux erfolgt über einen Befehl im Terminal. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind. Sie können ein Installationsskript vorbereiten und mit *sudo* ausführen.

Beispiel
(Neue Zeilen sind durch "\" unterbrochen, damit der gesamte Befehl ins Terminal kopiert werden kann.)

```
sudo ./Server-Linux-i386.sh \
--skip-license \
--db-driver=MySQL \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=Admin123 \
--server-root-password=Admin123 \
--db-user-username=root \
--db-user-password=Admin123 \
--cert-hostname="10.1.179.46;Ubuntu64-bb;Ubuntu64-bb.BB.LOCAL"
```

Der ERA-Server und der `eraserver`-Dienst werden an folgendem Speicherort installiert:
/opt/eset/RemoteAdministrator/Server

Sie können folgende Attribute ändern:

Attribut	Beschreibung	Erforderlich
--uninstall	Deinstalliert das Produkt	-

Attribut	Beschreibung	Erforderlich
--locale	Die Gebietsschema-ID (LCID) des installierten Servers (Standardwert: „en_US“). Siehe unterstützte Sprachen für mögliche Optionen. **Hinweis:** Sie können für jede ERA Web-Konsolen-Sitzung eine Sprache festlegen.	Ja
--skip-license	Der Benutzer wird während der Installation nicht zur Bestätigung der Lizenzvereinbarung aufgefordert.	
--skip-cert	Die Zertifikaterzeugung wird übersprungen (bitte zusammen mit dem Parameter --server-cert-path verwenden).	
--license-key	ESET-Lizenzschlüssel. Kann später festgelegt werden.	Nein
--product-guid	Globale eindeutige ID des Produkts. Wird erzeugt, falls nicht festgelegt.	Nein
--server-port	ESET Remote Administrator (ERA)-Serverport (Standardwert: 2222)	Nein
--console-port	Port für die ESET Remote Administrator-Konsole (Standardwert: 2223)	Nein
--server-root-password	Passwort für die Anmeldung bei der Web-Konsole mit dem Benutzer „Administrator“; mindestens 8 Zeichen lang.	Ja
--db-type	Art der Datenbank, die verwendet wird (mögliche Werte: „MySQL Server“, „Microsoft SQL Server“)	
--db-driver	ODBC-Treiber für die Verbindung zur Datenbank (z. B. „MySQL ODBC 5.3 ANSI Driver“)	Ja
--db-hostname	Computername oder IP-Adresse des Datenbankservers	Ja
--db-port	Port für den Datenbankserver (Standardwert: 3306)	Ja
--db-name	Name der Datenbank des ERA-Servers (Standardwert: „era_db“)	Ja
--db-admin-username	Benutzername des Datenbankadministrators (wird während der Installation zum Erstellen und Ändern der Datenbank verwendet)	Ja
--db-admin-password	Passwort des Datenbankadministrators	Ja
--db-user-username	Benutzername des ERA-Server-Datenbankbenutzers (wird vom ERA-Server für die Verbindung zur Datenbank verwendet); maximal 16 Zeichen	Ja
--db-user-password	Passwort für den Datenbankbenutzer des ERA-Servers	Ja
--cert-hostname	Enthält alle möglichen Namen und/oder IP-Adressen des Computers, auf dem der ERA-Server installiert wird. Dies muss mit dem Servernamen übereinstimmen, der im Zertifikat des Agenten angegeben ist, der über den Server eine Verbindung aufbaut.	Ja
--server-cert-path	Pfad zum Server-Peerzertifikat (verwenden Sie diese Option auch, wenn Sie --skip-cert angegeben haben)	
--server-cert-password	Passwort für das Server-Peerzertifikat	
--agent-cert-password	Passwort für das Agenten-Peerzertifikat	
--cert-auth-password	Passwort der Zertifizierungsstelle	
--cert-auth-path	ist der Pfad zur Zertifikatsbehördendatei des Servers	
--cert-auth-common-name	Allgemeiner Name der Zertifizierungsstelle (Anführungszeichen "" verwenden)	
--cert-organizational-unit	-	
--cert-organization	-	
--cert-locality	-	

Attribut	Beschreibung	Erforderlich
--cert-state	-	
--cert-country	-	
--cert-validity	Zertifikatgültigkeit in Tagen oder Jahren (im Argument --cert-validity-unit festlegen)	
--cert-validity-unit	Einheit für die Zertifikatgültigkeit; mögliche Werte sind „Years“ (Jahre) und „Days“ (Tage); Standardwert: Jahre	
--ad-server	Active Directory-Server	Nein
--ad-user-name	Name des Benutzers, der zum Durchsuchen des AD-Netzwerks berechtigt ist	Nein
--ad-user-password	Active Directory-Benutzerpasswort	Nein
--ad-cdn-include	Active Directory-Baumpfad für die Synchronisierung; leere Anführungszeichen "" verwenden, um den gesamten Baum zu synchronisieren	Nein

Installationsprogramm-Log

Der Log des Installationsprogramms kann für die Fehlersuche hilfreich sein. Er befindet sich unter folgendem Pfad:
`/var/log/eset/RemoteAdministrator/EraServerInstaller.log`

Überprüfen Sie nach der Installation, ob der Dienst „ERA-Server“ ausgeführt wird:
`service eraserver status`

3.8.1.1 Servervoraussetzungen – Linux

Zur Installation des ERA-Servers unter Linux müssen folgende Voraussetzungen erfüllt sein:

- Eine gültige Lizenz ist vorhanden.
- Ein Datenbankserver muss installiert und konfiguriert sein. Es ist ein Root-Konto erforderlich (vor der Installation muss kein Benutzerkonto erstellt werden, dieses kann vom Installationsprogramm erstellt werden).
- Ein ODBC-Treiber zur Verbindung mit dem Datenbankserver (MySQL / MS SQL) ist auf dem Computer installiert.
  `apt-get install unixodbc libmyodbc` (Debian, Ubuntu-Distributionen)
  `yum install mysql-connector-odbc` (CentOS, Red-Hat, Fedora-Distributionen)

HINWEIS: Verwenden Sie das Paket **unixODBC_23** (anstelle des standardmäßigen unixODBC), um eine problemlose Verbindung zwischen ERA-Server und MySQL-Datenbank zu gewährleisten. Dies gilt besonders für Installationen unter SUSE Linux.

- Die Serverinstallationsdatei ist als ausführbares Programm festgelegt.
  `chmod +x Server-Linux-i686.sh`
- Die niedrigste unterstützte Version von openSSL ist **openssl-1.0.1e-30**
- Auf Linux-Serversystemen ohne grafische Benutzeroberfläche wird für das ordnungsgemäße Drucken von Berichten (Bericht generieren) das Paket **xvfb** benötigt.
  `apt-get install xvfb` (Debian, Ubuntu)
  `yum install xorg-x11-server-Xvfb` (CentOS, Red-Hat, Fedora-Distributionen)
- Für die ordnungsgemäße Agenten-Bereitstellung auf Windows-Betriebssystemen wird das Paket **cifs-utils** benötigt.
  `apt-get install cifs-utils` (Debian, Ubuntu-Distributionen)
  `yum install cifs-utils` (CentOS, Red-Hat, Fedora-Distributionen)
- Die **Qt4 WebKit-Bibliotheken**: zum Drucken von Berichten im PDF- und PS-Format (muss Version 4.8 sein, nicht 5). Alle anderen **Qt4**-Abhängigkeiten werden automatisch installiert.
  `apt-get install libqtwebkit4` (Ubuntu-Distributionen)

HINWEIS: Für CentOS existiert in den offiziellen Repositories evtl. kein Paket. Installieren Sie das Paket aus einem externen Repository (z. B. EPEL-Repositories) oder kompilieren Sie es selbst auf einem Zielcomputer.

- Die Befehle **kinit + klist** für die Kerberos-Authentifizierung während des AD-Synchronisierungstasks und bei der Anmeldung mit einem Domänenbenutzer. Eine korrekte Kerberos-Konfiguration wird ebenfalls benötigt (*/etc/krb5.conf*).
  `apt-get install krb5-user` (Debian, Ubuntu-Distributionen)
  `yum install krb5-workstation` (CentOS, Red-Hat, Fedora-Distributionen)

- Die Befehle **wbinfo + ntlm_auth** für die Authentifizierung mit Domänenkonten + NTLM-Authentifizierung beim SMTP-Server (E-Mail-Versand)
  `apt-get install winbind` (Debian, Ubuntu-Distributionen)
  `yum install samba-winbind-clients` (CentOS, Red-Hat, Fedora-Distributionen)

- Der **ldapsearch**-Befehl für den AD-Synchronisierungstask.
  `apt-get install ldap-utils` (Debian, Ubuntu-Distributionen)
  `yum install openldap-clients` (CentOS, Red-Hat, Fedora-Distributionen)

- Der **snmptrap**-Befehl zum Senden von SNMP-Traps. Optional, falls diese Funktion nicht verwendet wird. SNMP muss ebenfalls konfiguriert werden.
  `apt-get install snmp` (Ubuntu-Distributionen)
  `yum install net-snmp-utils` (CentOS, Red-Hat, Fedora-Distributionen)

- Das **SELinux devel-Paket**, das bei der Produktinstallation zur Erstellung von SELinux-Policy-Modulen verwendet wird. Wird nur auf Systemen mit aktiviertem SELinux benötigt (CentOS, Fedora, RHEL).
  `apt-get install selinux-policy-dev` (Debian, Ubuntu-Distributionen)
  `yum install policycoreutils-devel` (CentOS, Red-Hat, Fedora-Distributionen)

HINWEIS: Der ERA-Server speichert große Datenblöcke in der Datenbank. Daher muss MySQL zur Annahme großer Paketgrößen konfiguriert sein, damit ERA ordnungsgemäß funktioniert. Ausführliche Informationen zu dieser Konfiguration finden Sie in unseren FAQ.

3.8.2 Agenten-Installation – Linux

Für die Verbindung zum ERA-Server werden die Parameter „--hostname“ und „--port“ verwendet („--port“ wird nur verwendet, wenn kein SRV-Eintrag angegeben wird). Mögliche Verbindungsformate:

- **Hostname** und **Port**
- **IPv4-Adresse** und **Port**
- **IPv6-Adresse** und **Port**
- Diensteintrag (SRV-Eintrag) - Zur Konfiguration des DNS-Ressourceneintrags unter Linux muss sich der Computer in der Domäne eines funktionierenden DNS-Servers befinden. Siehe DNS-Ressourceneintrag.

Der SRV-Eintrag muss mit dem Präfix „_NAME._tcp“ beginnen. „NAME“ stellt einen benutzerdefinierten Namen dar (zum Beispiel „era“).

Unten sehen Sie ein Beispiel für einen Installationsskript. Die Skriptparameter werden im folgenden Abschnitt beschrieben.

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/admin/Desktop/agent.pfx --cert-auth-path=/h
--cert-password=N3lluI4#2aCC --hostname=10.1.179.36 --port=2222
```

`--skip-license` verhindert, dass das Installationsprogramm den Benutzer zur Bestätigung der Lizenz auffordert
`--cert-path` ist der Pfad zur Agenten-Zertifikatdatei
`--cert-auth-path` ist der Pfad zur Zertifikatsbehördendatei des Servers
`--cert-password` muss mit dem Zertifikats-Passwort des Agenten übereinstimmen
`--hostname` ist eine Verbindung zu einem Server (oder Proxy) in einem dieser Formate (Hostname, IPv4, IPv6 oder SRV-Datensatz)
`--port` ist ein überwachender, offener Port auf dem Server oder Proxy (der Standardwert ist für beide 2222)

Optionale Parameter:
Produkt-GUID (wird generiert, falls nicht angegeben)
`--cert-content` Base64-codierter Inhalt des PKCS12-codierten Zertifikats für den öffentlichen Schlüssel plus der private Schlüssel, der für die Einrichtung sicherer Kommunikationskanäle mit Servern und Agenten verwendet wird. Verwenden Sie nur eine der Optionen `--cert-path` oder `--cert-content`.
`--cert-auth-content`Base64-codierter Inhalt des DER-codierten privaten Zertifikats der Zertifizierungsstelle zur Verifizierung von Remote-Rechnern (Proxy oder Server). Verwenden Sie nur eine der Optionen
oder `--cert-auth-content`.
Der Hostname, den die Web-Konsole für die Verbindung zum Server verwendet (wird aus „hostname" kopiert, falls leer)
Der Port, den die Web-Konsole für die Verbindung zum Server verwendet (Standardwert: 2223)
`--webconsole-user` Der Benutzername, den die Web-Konsole für die Verbindung zum Server verwendet (Standardwert: „Administrator")
`--webconsole-password` Das Passwort, das die Web-Konsole für die Verbindung zum Server verwendet

Verbindung und Zertifikate

- **Verbindung zum ERA-Server** muss angegeben werden: (Port wird nicht benötigt, wenn ein Diensteintrag angegeben wurde, der Standardwert ist 2222)
- Geben Sie diese Verbindungsdaten für die **servergestützte Installation** an: --webconsole-port, --webconsole-user, --webconsole-password
- Geben Sie Zertifikatsinformationen für die **Offline-Installation** an: `--cert-path, --cert-password`

Passwort-Typ-Parameter

Passwort-Typ-Parameter können als Umgebungsvariablen oder in einer Datei angegeben, aus stdin gelesen oder als Nur-Text angegeben werden:
`--password=env:SECRET_PASSWORD` wobei SECRET_PASSWORD eine Umgebungsvariable mit dem Passwort ist
`--password=file:/opt/secret` wobei die erste Zeile der regulären Datei /opt/secret das Passwort enthält
`--password=stdin` weist das Installationsprogramm an, das Passwort aus der Standardeingabe zu lesen
`--password="pass:PASSWORD"` entspricht `--password="PASSWORD"` und muss angegeben werden, falls das Passwort gleich `"stdin"` ist oder eine Zeichenfolge beginnend mit `"env:"`, `"file:"` oder `"pass:"`

Installationsprogramm-Log

Der Log des Installationsprogramms kann für die Fehlersuche hilfreich sein. Er befindet sich unter folgendem Pfad:
`/var/log/eset/RemoteAdministrator/EraAgentInstaller.log`

Um zu überprüfen, ob die Installation erfolgreich war, überprüfen Sie, ob der Dienst ausgeführt wird. Führen Sie dazu folgenden Befehl aus:
```
sudo service eraagent status
```

3.8.2.1 Voraussetzungen für Agenten – Linux

Zur Installation des ERA-Agenten unter Linux müssen folgende Voraussetzungen erfüllt sein:

- Der ERA-Server und die ERA Web-Konsole müssen installiert sein
- Für den Agenten muss ein Zertifikat vorhanden sein.
- Ein Datei mit dem öffentlichen Schlüssel der Zertifizierungsstelle des Servers muss vorhanden sein.
- Der Servercomputer muss über das Netzwerk erreichbar sein.
- Die Installationsdatei für den Agenten muss als ausführbare Datei festlegt sein (führen Sie hierzu den Befehl „chmod +x" für die Datei aus)
- Die niedrigste unterstützte Version von openssl ist **openssl-1.0.1e-30**.

3.8.3 Installation der ERA Web-Konsole – Linux

Stellen Sie vor der Installation der ERA Web-Konsole sicher, dass alle Voraussetzungen erfüllt sind:

1. Führen Sie die folgenden Befehle aus, um die Datei „era.war“ in den ausgewählten Ordner zu kopieren:
   `sudo cp era.war /var/lib/tomcat7/webapps/`
   Alternativ können Sie den Inhalt von era.war nach `/var/lib/tomcat7/webapps/era/` extrahieren

2. Führen Sie den folgenden Befehl aus, um den tomcat-Dienst neu zu starten und die .war-Datei bereitzustellen, z. B.:
   `sudo service tomcat7 restart`

3. Öffnen Sie den folgenden Link in einem Browser auf dem Localhost (ein Anmeldebildschirm wird angezeigt):
   http://localhost:8080/era

HINWEIS: Wenn Sie die Web-Konsole mit dem Installationsprogramm installieren, lautet die standardmäßige Adresse der Web-Konsole:

https://localhost/era/

3.8.3.1 Voraussetzungen für die ERA Web-Konsole – Linux

Zur Installation der ERA-Web-Konsole unter Linux müssen folgende Voraussetzungen erfüllt sein:

- Java - Verwenden Sie immer die aktuellste Java-Version (Obwohl die ERA Web-Konsole mindestens Java Version 7 benötigt, empfehlen wir dringend die Verwendung der aktuellsten offiziellen Java-Version)
  `apt-get install openjdk-7-jdk` (Debian, Ubuntu-Distributionen)
  `yum install java-1.8.0-openjdk` (Red-Hat, Fedora)

- Apache Tomcat (Version 6 und höher)
  `sudo apt-get install tomcat7`
  `yum install tomcat7`

- Datei der Web-Konsole (*era.war*) auf der lokalen Festplatte gespeichert.

3.8.4 Proxyserverinstallation – Linux

1. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind.
2. Führen Sie zur Installation des Proxyservers ein Installationsskript aus. Nachstehend finden Sie ein Beispiel eines solchen Installationsskripts.

Verbindungseinstellungen

Ein Ziel muss mit folgenden Angaben angegeben werden:

- Hostname
- IPv4-Adresse
- IPv6-Adresse
- DNS-Ressourceneintrag – Der Linux-Computer muss sich in der Domäne befinden. Siehe Kapitel DNS-Ressourceneintrag.

Der Port muss festgelegt sein: Verwenden Sie Port 2222 für den Server und den Proxy.

Installationsbeispiel
(Neue Zeilen sind durch "\" unterbrochen, damit der gesamte Befehl ins Terminal kopiert werden kann.)

```
./Proxy-Linux-x86_64-1.0.407.0.sh --db-hostname=10.1.179.28 --db-dbname=era_6_db_proxy \
--db-admin-username=sa --db-admin-password=admin.1 --db-user-username=tester \
--db-user-password=Admin.1 --db-port=1433 --db-type="MS SQL Server" \
--db-driver=SQL --skip-license --hostname=10.1.179.30 --port=2222 \
--cert-path=/home/adminko/Desktop/proxy.pfx --cert-auth-path=/home/adminko/Desktop/CA-server.der \
--cert-password=root --server-root-password=jjf#jDjr
```

Sie können folgende Attribute ändern:

ist ein Hostname oder die IP-Adresse des DB-Servers
ist der Name der verwendeten Datenbank
ist der Name eines DB-Administrators
ist das Passwort des DB-Administrators
ist ein Benutzer für den Zugriff auf die Datenbank
ist das Passwort dieses Benutzers
ist der Port für die Datenbank (1433 für MSSQL, 3306 für MySQL)
ist die Definition des verwendeten Datenbanktyps (mögliche Werte sind „MySQL Server“ und „MS SQL Server“)
muss auf den gleichen Namen festgelegt sein wie für MSSQL in
fordert den Benutzer nicht zur Bestätigung der Lizenz auf
ist ein Hostname oder die IP-Adresse des Servers
`--port` ist der Serverport (standardmäßig 2222) bzw. Proxy-Port (standardmäßig 1236)
Der vom Proxy verwendete Port (standardmäßig 2222)
ist ein lokaler Pfad zur Proxy-Zertifikatsdatei
ist ein lokaler Pfad zur Datei der Zertifizierungsstelle des Servers
diese Einstellung ist wichtig und muss angegeben werden, wenn Sie MySQL verwenden. Wenn diese Einstellung nicht festgelegt ist, wird der MySQL-Standardport 3306 verwendet.
Produkt-GUID (wird generiert, falls nicht angegeben)
`--cert-content` Base64-codierter Inhalt des PKCS12-codierten Zertifikats für den öffentlichen Schlüssel plus der private Schlüssel, der für die Einrichtung sicherer Kommunikationskanäle mit Servern und Agenten verwendet wird.
Verwenden Sie nur eine der Optionen `--cert-path` oder `--cert-content`.
muss mit dem Zertifikats-Passwort des Agenten übereinstimmen
Base64-codierter Inhalt des DER-codierten privaten Zertifikats der Zertifizierungsstelle zur Verifizierung von Remote-Rechnern (Proxy oder Server). Verwenden Sie nur eine der Optionen
oder `--cert-auth-content`.
`--keep-database` Die Datenbank wird bei der Deinstallation nicht entfernt

Mit dem folgenden Befehl können Sie überprüfen, ob der Dienst ausgeführt wird und die Installation somit erfolgreich war:

```
sudo service eraproxy status
```

3.8.4.1 Proxyservervoraussetzungen – Linux

Zur Installation der ERA-Proxykomponente unter Linux müssen folgende Voraussetzungen erfüllt sein:

- **Der ERA-Server** und die **ERA Web-Konsole** sind installiert (auf einem Servercomputer).
- Ein ODBC-Treiber zur Verbindung mit dem Datenbankserver (MySQL / MS SQL) ist auf dem Computer installiert.
- Ein Datenbankserver ist bereits installiert und konfiguriert.
- Ein **Proxyzertifikat** ist erstellt und wurde zum lokalen Laufwerk heruntergeladen.
- Eine **Zertifizierungsstelle** ist auf dem lokalen Laufwerk vorbereitet.
- Eine gültige Lizenz ist vorhanden.
- Der Agent muss auf einem lokalen Computer installiert sein, damit alle Programmfunktionen vollständig unterstützt werden.
- Die niedrigste unterstützte Version von openssl ist **openssl-1.0.1e-30**.

3.8.5 Rogue Detection Sensor-Installation und Voraussetzungen – Linux

Führen Sie diese Schritte aus, um RD Sensor unter Linux zu installieren:

1. Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind:
   - Das Netzwerk muss durchsucht werden können (Ports sind geöffnet, die Firewall blockiert die eingehende Kommunikation nicht usw.).
   - Der Servercomputer ist erreichbar.
   - Der ERA-Agent muss auf dem lokalen Computer installiert sein, damit alle Programmfunktionen vollständig unterstützt werden.
   - Das Terminal ist offen.
2. Mit folgendem Befehl können Sie die Installationsdatei als sudo ausführen:

```
sudo ./RDSensor-Linux-x86_64-1.0.223.0.sh
```

3. Um zu überprüfen, ob die Installation erfolgreich war, überprüfen Sie, ob der Dienst ausgeführt wird. Führen Sie dazu den folgenden Befehl aus:

```
sudo service rdsensor status
```

4. Rogue Detection Sensor wird auf Ihrem Computer installiert.
5. Die Log-Datei des Rogue Detection Sensor befindet sich unter folgendem Pfad: *var/log/eset/RemoteAdministrator/RogueDetectionSensor/trace.log*

3.8.6 Installation des Connectors für Mobilgeräte - Linux

Sie können den Connector für Mobilgeräte auf einem anderen Server installieren, als der Server, auf dem der ERA-Server ausgeführt wird. Dies ist beispielsweise sinnvoll, wenn über das Internet auf den Connector für Mobilgeräte zugegriffen werden soll, um jederzeit die Mobilgeräte der Benutzer verwalten zu können.

Die Installation der ERA-Serverkomponente unter Linux erfolgt über einen Befehl im Terminal. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind. Sie können ein Installationsskript vorbereiten und mit *sudo* ausführen.

Es stehen viele optionale Installationsparameter zur Verfügung, einige sind jedoch erforderlich.

Für die Installation benötigen Sie Ihr ERA-Peerzertifikat. Das ERA-Peerzertifikat kann auf zwei verschiedene Weisen abgerufen werden:

- **Servergestützte Installation** - Hierzu müssen Sie die Anmeldedaten des Administrators der ERA-Webkonsole eingeben (das Installationsprogramm lädt automatisch die erforderlichen Zertifikate herunter).
- **Offline-Installation** - Hierzu müssen Sie ein Peerzertifikat angeben (das Agentenzertifikat, das Sie aus ESET Remote Administrator exportiert haben). Alternativ können Sie ein benutzerdefiniertes Zertifikat verwenden.

Folgende Parameter müssen für den Installationsbefehl angegeben werden:

HTTPS-Zertifikat:

```
--https-cert-path=
--https-cert-password=
```

Peerzertifikat:
Bei einer **servergestützten Installation** muss mindestens Folgendes enthalten sein:

```
--webconsole-password=
```

Bei einer **Offline-Installation** Folgendes angeben:

`--cert-path=`

`--cert-password=` (Für das standardmäßige Agentenzertifikat, das bei der Erstinstallation des ERA-Servers erstellt wird, ist kein Passwort erforderlich)

Verbindung zum ERA-Server (Name oder IP-Adresse):

```
--hostname=
```

Für eine MySQL-Datenbank Folgendes angeben:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Für eine MSSQL-Datenbank Folgendes angeben:

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Wenn eine MySQL-/MSSQL-Datenbank bereits vorhanden ist, einen der beiden folgenden Befehle angeben:

```
--db-use-existing-db=
```

oder

```
--db-drop-existing-db=
```

Beispiel

(Neue Zeilen sind durch "\" unterbrochen, damit der gesamte Befehl ins Terminal kopiert werden kann.)

```
sudo ./MDMCore-Linux-x86_64-0.0.0.0.sh \
--https-cert-path="./httpscert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--db-use-existing-db \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

Mit folgendem Befehl erhalten Sie die vollständige Liste aller verfügbaren Parameter (Hilfemeldung drucken):

```
--help
```

Installationsprogramm-Log

Der Log des Installationsprogramms kann für die Fehlersuche hilfreich sein. Er befindet sich unter folgendem Pfad:

```
/var/log/eset//mdminstaller.log
```

Überprüfen Sie nach dem Abschluss der Installation, ob der Connector für Mobilgeräte richtig ausgeführt wird. Öffnen Sie hierzu in einem Webbrowser die Adresse 'https://*ihr-mdm-hostname*:*registrierungs-port* (zum Beispiel *https://eramdm:9980*). Wenn die Installation erfolgreich war, wird folgende Meldung angezeigt:

eset REMOTE ADMINISTRATOR

MDM Server up and running!

Sie können diese URL außerdem dazu verwenden, um die Verfügbarkeit des Connectors für Mobilgeräte aus dem Internet zu überprüfen (sofern so konfiguriert), indem Sie mit einem Mobilgeräte auf die URL zugreifen. Wenn Sie die Seite nicht erreichen können, überprüfen Sie die Firewall und die Konfiguration der Netzwerkinfrastruktur.

3.8.6.1 Voraussetzungen für den Connector für Mobilgeräte - Linux

Zur Installation des Connectors für Mobilgeräte unter Linux müssen folgende Voraussetzungen erfüllt sein:

- Ein Datenbankserver muss installiert und konfiguriert sein. Es ist ein Root-Konto erforderlich (vor der Installation muss kein Benutzerkonto erstellt werden, dieses kann vom Installationsprogramm erstellt werden).
- Ein ODBC-Treiber zur Verbindung mit dem Datenbankserver (MySQL / MS SQL) ist auf dem Computer installiert.
  `apt-get install unixodbc libmyodbc` (Debian, Ubuntu-Distributionen)
  `yum install mysql-connector-odbc` (CentOS, Red-Hat, Fedora-Distributionen)

HINWEIS: Verwenden Sie das Paket **unixODBC_23** (anstelle des standardmäßigen unixODBC), um eine problemlose Verbindung zwischen dem ERA-Server und der MySQL-Datenbank zu gewährleisten. Dies gilt besonders für Installationen unter SUSE Linux.

- Die Serverinstallationsdatei ist als ausführbares Programm festgelegt.
  `chmod +x MDMCore-Linux-i686.sh`
- Überprüfen Sie nach der Installation, ob der Dienst MDMCore ausgeführt wird.
  `service mdmcore status`
- Die niedrigste unterstützte Version von openSSL ist **openssl-1.0.1e-30**

HINWEIS: Der ERA-Server speichert große Datenblöcke in der Datenbank. Daher muss MySQL zur Annahme großer Paketgrößen konfiguriert sein, damit ERA ordnungsgemäß funktioniert. Ausführliche Informationen zu dieser Konfiguration finden Sie in unseren FAQ.

WICHTIG: Sie benötigen ein **SSL-Zertifikat** im `.pfx` -Format, um eine sichere Verbindung über HTTPS herstellen zu können. Wir empfehlen die Verwendung eines von einer Zertifizierungsstelle bereitgestellten Zertifikats. Selbstsignierte Zertifikate werden nicht empfohlen, da einige Mobilgeräte dem Benutzer nicht die Möglichkeit bieten, selbstsignierte anzunehmen. Bei der Verwendung von Zertifikaten, die von einer Zertifizierungsstelle signiert sind, stellt dies kein Problem dar, weil diese Zertifikate vertrauenswürdig sind und keine Annahme durch den Benutzer erforderlich ist.

WICHTIG: Für die Offline-Installation benötigen Sie außerdem ein Peerzertifikat (das **Agentenzertifikat**, das Sie aus ESET Remote Administrator exportiert haben). Alternativ können Sie mit ERA ein benutzerdefiniertes Zertifikat verwenden.

3.8.7 Apache HTTP Proxy-Installation – Linux

Führen Sie die folgenden Schritte aus, um die Apache HTTP-Proxy-Komponente unter Windows zu installieren:

1. Installieren Sie den Apache HTTP-Server (mindestens Version 2.4.10)
2. Laden Sie die folgenden Module: access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile, authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk
3. Fügen Sie die Caching-Konfiguration hinzu:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Falls das Verzeichnis */var/cache/apache2/mod_cache_disk* nicht existiert, erstellen Sie es und erteilen Sie Apache die Berechtigungen (r,w,x)
5. Fügen Sie die Proxy-Konfiguration hinzu:

```
ProxyRequests On
ProxyVia On
```

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Aktivieren Sie die hinzugefügte Konfiguration (überspringen Sie diesen Schritt, falls sich die Konfiguration in der Haupt-Konfiguration befindet)
7. Ändern Sie bei Bedarf den Listening-Port (standardmäßig ist Port 3128 eingestellt)
8. Optionale Standardauthentifizierung:
   - Fügen Sie die Authentifizierungskonfiguration zur Proxy-Anweisung hinzu:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

   - Erstellen Sie eine Passwortdatei mit dem Befehl `htpasswd.exe -c`
   - Erstellen Sie manuell eine Datei mit dem Namen group.file mit dem Befehl `usergroup:username`
9. Starten Sie den Server neu

Ubuntu Server 14.10:

1. `sudo apt-get install apache2`
2. `sudo a2enmod access_compat auth_basic authn_core authn_file authz_core authz_groupfile \`
   `authz_host proxy proxy_http proxy_connect cache cache_disk`
3. `sudo vim /etc/apache2/conf-available/caching.conf`
   - Fügen Sie die Caching-Konfiguration ein:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Dieser Schritt wird normalerweise nicht benötigt. Falls jedoch das Caching-Verzeichnis fehlt, führen Sie die folgenden Befehle aus:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. `sudo vim /etc/apache2/conf-available/proxy.conf`
   - Fügen Sie die Proxy-Konfiguration ein:

```
ProxyRequests On
ProxyVia On

<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. `sudo a2enconf caching.conf proxy.conf`
7. `sudo vim /etc/apache2/ports.conf`
   - Ersetzen Sie `Listen 80` durch `Listen 3128`
8. Optionale Standardauthentifizierung:

o `sudo vim /etc/apache2/conf-available/proxy.conf`

Fügen Sie die Authentifizierungs-Konfiguration vor `</Proxy>` ein:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

```
sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user
sudo vim /etc/apache2/group.file
insert: usergroup:user
```

9. `sudo service apache2 restart`

Allgemeine Einstellungen:

Weiterleitung nur für ESET-Kommunikation erlauben:

1. Ersetzen Sie in der Proxy-Konfiguration den Block:

```
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

durch:

```
<Proxy *>
Deny from all
</Proxy>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\. \
[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\. \
[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2. \
mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net|edf-pcs.cloudapp.net|edf-pcs2.clouda
edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
<ProxyMatch ^[h,H][t,T][t,T][p,P][s,S]?://([^@/]*@)?(87.106.247.14|209.157.66.250|209.157.66.253| \
212.227.134.125|212.227.134.126|212.227.134.128|212.227.134.130|212.227.134.131|212.227.134.132| \
212.227.134.133|212.227.134.158)(:[0-9]+)?(/.*)?$>
Allow from all
</ProxyMatch>
```

Proxy-Verkettung (sämtlicher Datenverkehr):

Fügen Sie die folgende Zeile zur Proxy-Konfiguration hinzu (Passwort funktioniert nur für untergeordneten Proxy):

```
ProxyRemote * http://10.1.172.26:3128
```

Squid3:

1. Installieren Sie Squid3
2. Fügen Sie `cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000` zu Ihrer Konfiguration unter `cache_dir` hinzu (5000 ist die Cachegröße in MB)
3. Erstellen Sie einen Cachingordner mit Squid: `squid3 -z` (beenden Sie den squid3-Dienst, falls dieser läuft)
4. Gestatten Sie den Zugriff für die gewünschten Clients
5. Starten Sie squid3 neu

Ubuntu Server 14.10:

1.`sudo apt-get install squid3`

2.`sudo vim /etc/squid3/squid.conf`

Ersetzen Sie `#cache_dir ufs /var/spool/squid3 100 16 256` durch `cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000`

3.`sudo service squid3 stop`

`sudo squid3 -z`

4.`sudo vim /etc/squid3/squid.conf`

Fügen Sie `http_access allow all` vor `http_access deny all` ein, um den Proxyzugriff allgemein zu gestatten

5.`sudo service squid3 restart`

3.8.8 Deinstallieren und Neuinstallieren einer Komponente – Linux

Zum Ausführen einer Neuinstallation oder einer Aufrüstung auf eine neuere Version führen Sie erneut das Installationsskript aus.

Zur Deinstallation einer Komponente (in diesem Fall der ERA-Server) führen Sie das Installationsprogramm wie nachfolgend gezeigt mit dem Parameter **--uninstall** aus:

```
sudo ./Server-Linux-i686.sh --uninstall --keep-database
```

Falls Sie andere Komponenten deinstallieren möchten, verwenden Sie den entsprechenden Paketnamen im Befehl. Für de

```
sudo ./Agent-Linux-x86_64.sh --uninstall
```

Warnung: Bei der Deinstallation werden Konfigurations- und Datenbankdateien gelöscht. Um die Datenbankdateien beizubehalten, erstellen Sie eine SQL-Sicherung der Datenbank oder verwenden Sie den Parameter `--keep-database`.

Prüfen Sie nach der Deinstallation Folgendes

- Der Dienst `eraserverService.sh` wurde gelöscht.
- Der Ordner `/etc/opt/eset/RemoteAdministrator/Server/` wurde gelöscht.

Es empfiehlt sich, vor der Deinstallation eine Datenbanksicherung auszuführen, falls Sie die Daten später wiederherstellen möchten.

3.9 DNS-Diensteintrag

So richten Sie einen DNS-Ressourceneintrag ein:

1. Navigieren Sie auf dem DNS-Server (DNS-Server im Domänencontroller) zu **Systemsteuerung** > **Verwaltung**.
2. Wählen Sie den DNS-Wert aus.
3. Wählen Sie im DNS Manager *_tcp* aus dem Baum aus und erstellen Sie einen neuen Eintrag für **Dienstidentifizierung (SRV)**.
4. Geben Sie den Dienstnamen im Feld **Dienst** ein. Beachten Sie dabei die DNS-Standardregeln und geben Sie vor dem Dienstnamen einen Unterstrich ein (**_**). Verwenden Sie einen eigenen Dienstnamen, z. B. **_era**.
5. Geben Sie das TCP-Protokoll im Feld **Protokoll** im folgenden Format ein: *_tcp*.
6. Geben Sie im Feld **Portnummer** den Port 2222 ein.
7. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) des ERA-Servers im Feld **Host, der diesen Dienst anbietet** ein.
8. Speichern Sie den Eintrag durch Klicken auf [**OK**] und klicken Sie dann auf [**Fertig**]. Der Eintrag wird in der Liste angezeigt.

So überprüfen Sie einen DNS-Eintrag:

1. Melden Sie sich an einem beliebigen Computer in der Domäne an und öffnen Sie die Eingabeaufforderung (*cmd.exe*).
2. Geben Sie in der Befehlszeile *nslookup* ein und drücken Sie die **Eingabetaste**.
3. Geben Sie *set querytype=srv* ein und drücken Sie die **Eingabetaste**.
4. Geben Sie *_era._tcp.domain.name* ein und drücken Sie die **Eingabetaste**. Die Dienstidentifizierung wird richtig angezeigt.

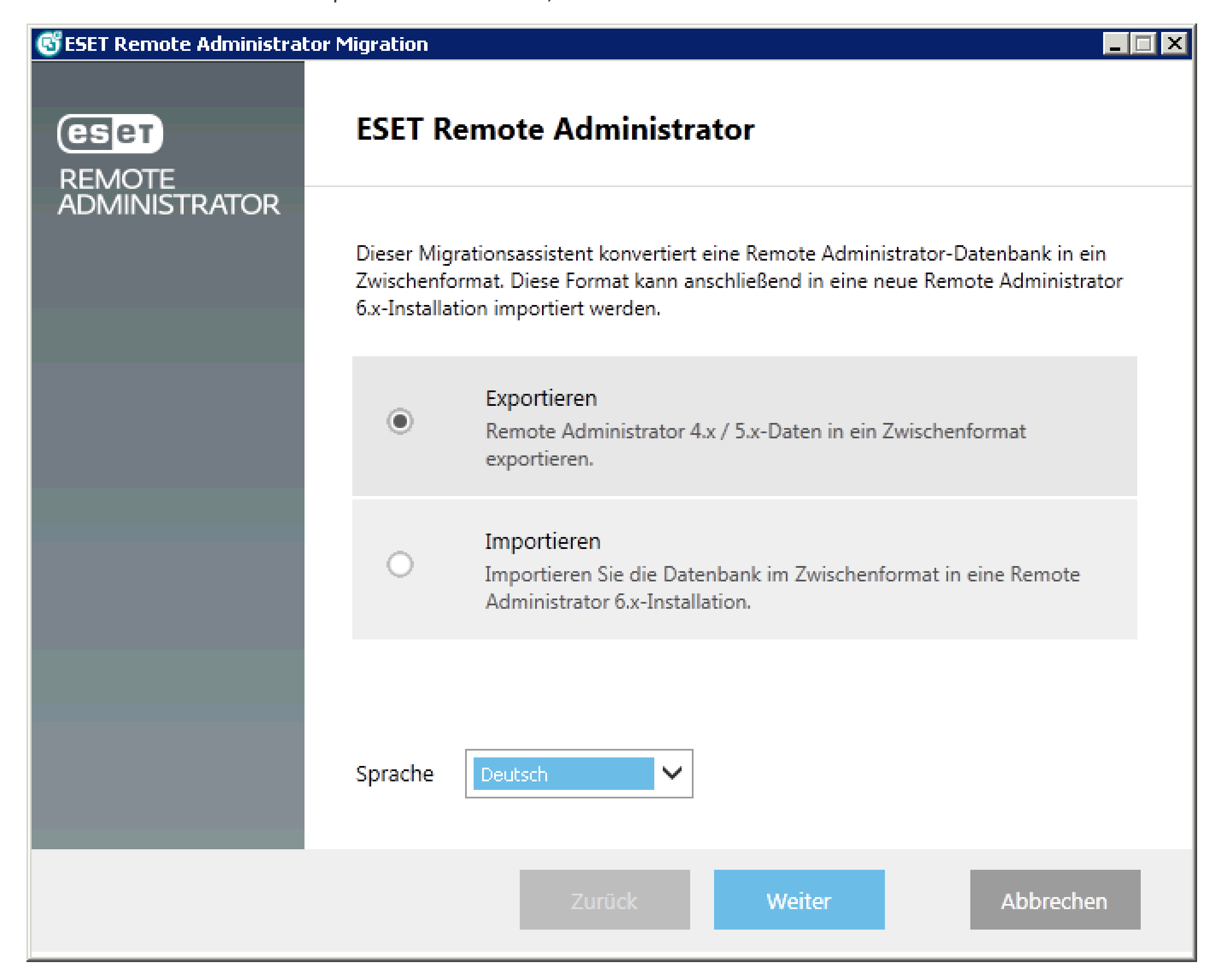
HINWEIS: Diese Prozedur gilt für Windows und Linux.

HINWEIS: Denken Sie daran, den Wert unter „Host, der diesen Dienst anbietet" in den FQDN des neuen Servers zu ändern, wenn Sie den ESET Remote Administrator-Server auf einem anderen Computer installieren.

3.10 Migrations-Tool

Der Migrationsassistent ist eine eigenständige Anwendung, mit der Sie Daten aus ERA 4.x/5.x bequem in eine vorübergehende Datenbank migrieren und anschließend in ERA 6.x importieren können.

Laden Sie das ESET Remote Administrator Migration Tool herunter. Sie benötigen einen von ESET ausgestellten Benutzernamen und das entsprechende Passwort, um das Tool herunterzuladen.



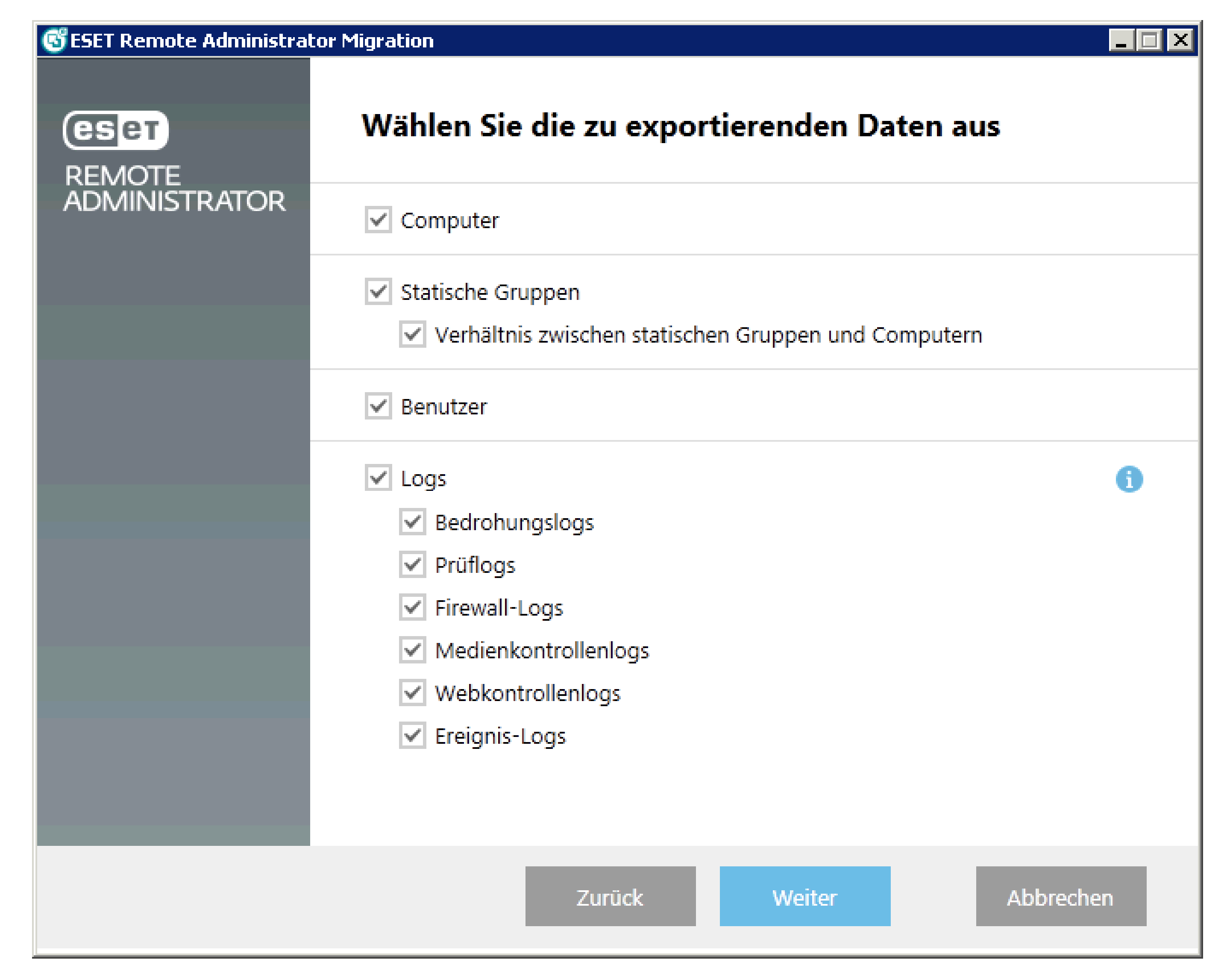
HINWEIS: Wenn ein Problem aufgrund einer fehlenden Datei `MSVCP100.dll` oder `MSVCR100.dll` auftritt, installieren Sie das neueste Microsoft Visual C++ 2010 Redistributable Package. Verwenden Sie hierzu folgenden Link: Microsoft

Visual C++ 2010 Redistributable Package (x86).

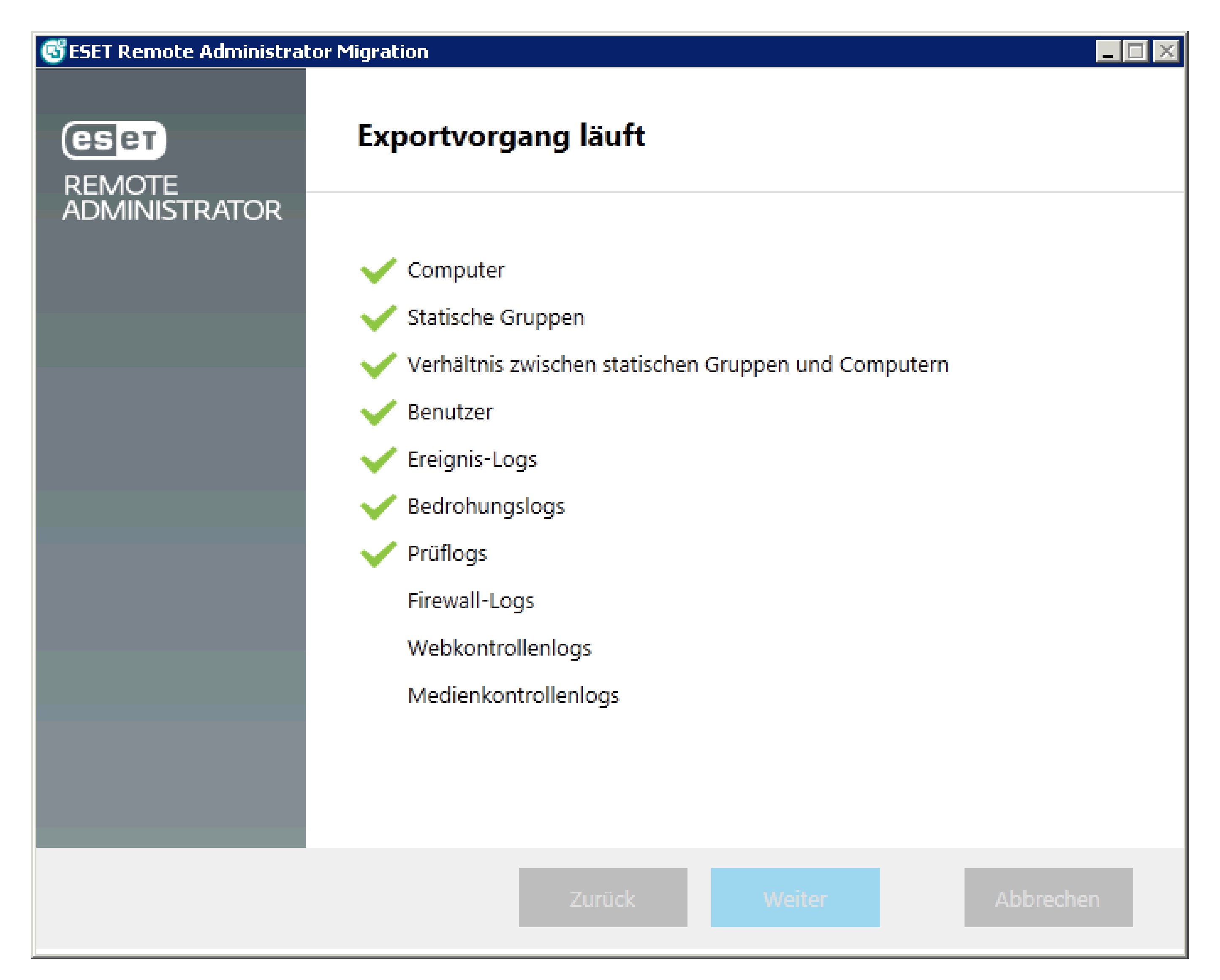
3.10.1 Migrationsszenario 1

Dieses Szenario gilt für die Migration auf ERA 6.x, das auf einem anderen Computer als ERA 4.x/5.x ausgeführt wird.

1. Als erster Schritt der Migration muss ERA 6.x auf einem anderen Computer installiert und ausgeführt werden.
2. Starten Sie das Migrations-Tool von ESET Remote Administrator auf dem Computer mit ERA 4.x/5.x und wählen Sie **Exportieren** aus, um die Daten von der alten ERA-Instanz in einer temporären Datenbankdatei zu speichern.
3. Der Migrationsassistent kann nur bestimmte Daten übertragen. Wählen Sie die zu übertragenden Daten aus und klicken Sie auf „Weiter".



Aufgrund des neuen Aufbaus und der neuen Funktion der dynamischen Gruppen in ERA 6.x können parametrische Gruppen, Tasks und Policies nicht aus früheren Versionen übertragen werden. Nachdem Sie einen Ordner zum Speichern der temporären Datenbank ausgewählt haben, zeigt der Assistent den Status der Archivierung der ERA 4.x/5.x-Datenbank an.



Alle Daten werden in eine **Zwischendatenbank** exportiert.

4. Nach dem Datenexport stehen zwei Optionen zur Verfügung:
   - Eine Möglichkeit besteht darin, den Export mit **Fertig stellen** abzuschließen, mit der Funktion **Kopieren** die temporäre Datenbankdatei zu einem Server kopieren, auf dem ESET Remote Administrator 6.x ausgeführt wird, und die Daten auf diesem Server mit dem ERA-Migrations-Tool importieren.
   - Alternativ können Sie auf **Jetzt importieren** klicken, um die Daten direkt über das Netzwerk zu ESET Remote Administrator 6.x zu importieren. Geben Sie die Verbindungs- und Anmeldedaten für den neuen ERA-Server an.

HINWEIS: Aus Active Directory synchronisierte statische Gruppen werden ignoriert und nicht exportiert.

- Wenn die Servereinstellungen das Importieren bestimmter Daten nicht zulassen, können Sie im Migrations-Tool von ESET Remote Administrator wählen, ob Sie die Einstellungen des ERA 6.x-Servers für bestimmte Komponenten ändern möchten.

- Die einzelnen Komponenten werden dann importiert. Für jede Komponente steht ein **Import-(Migrations-) Log** zur Verfügung. Nach dem Importieren zeigt das Migrations-Tool die Ergebnisse des Importprozesses an.

- Wenn Sie Benutzer migriert haben, wurden die Passwörter zurückgesetzt und durch zufällig erstellte Passwörter ersetzt. Diese Passwörter können im `csv` -Format exportiert werden.

- Der Assistent des Migrations-Tools generiert außerdem ein Skript, mit dem die ERA-Agenten auf den Clientcomputern vorkonfiguriert werden können. Das Skript ist eine kleine ausführbare `.bat` -Datei, die an die Clientcomputer verteilt werden kann.

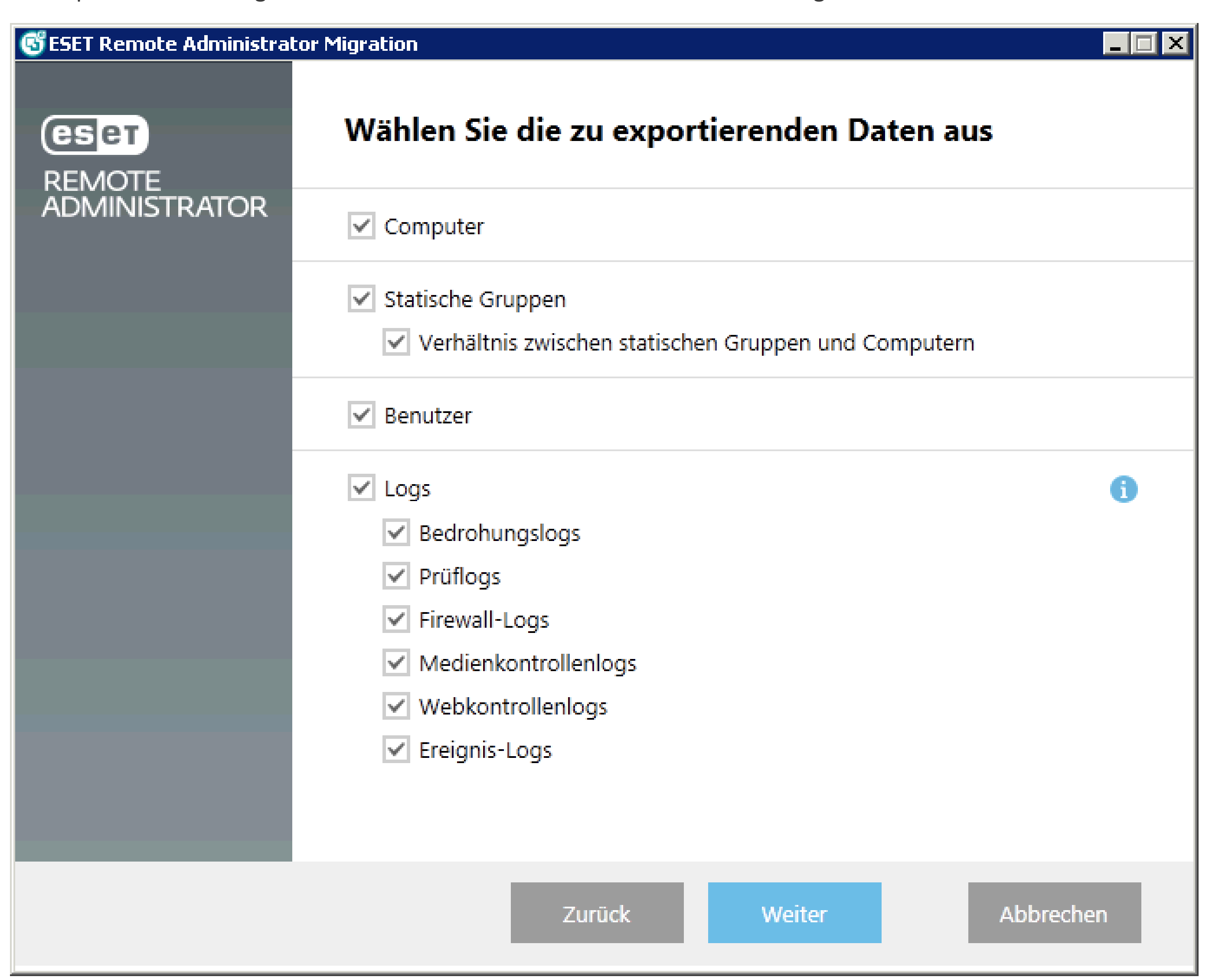
- Es empfiehlt sich, die migrierten Einstellungen und Daten zu überprüfen, um sicherzustellen, dass der Import erfolgreich ausgeführt wurde. Nach der Überprüfung können Sie das Skript zum Bereitstellen des ERA-Agenten auf einer begrenzten Zahl Computer verwenden, um zu überprüfen, ob die Verbindung zum Server richtig hergestellt wird.
- Wenn die Computer dieser Testgruppe erfolgreich eine Verbindung herstellen, können Sie den Agenten auf den verbleibenden Computern bereitstellen (entweder manuell oder mit einem AD-Synchronisierungstask).

HINWEIS: Wenn bei einem der Migrationsschritte ein Fehler auftritt, machen Sie die für ERA 6.x vorgenommenen Änderungen rückgängig, richten Sie die Computer zur Verbindung mit ERA 4.x/5.x ein, stellen Sie die Sicherungsdaten von ERA 4.x/5.x wieder her und wenden Sie sich an den ESET-Support.

3.10.2 Migrationsszenario 2

Dieses Szenario gilt für die Migration auf ERA Remote Administrator 6.x, das auf dem gleichen Computer wie ERA 4.x/5.x ausgeführt wird. Vor der Datenmigration sollten sämtliche ERA-Daten (mit dem ESET-Wartungs-Tool) gesichert und die verbundenen Dienste im Betriebssystem gestoppt werden.

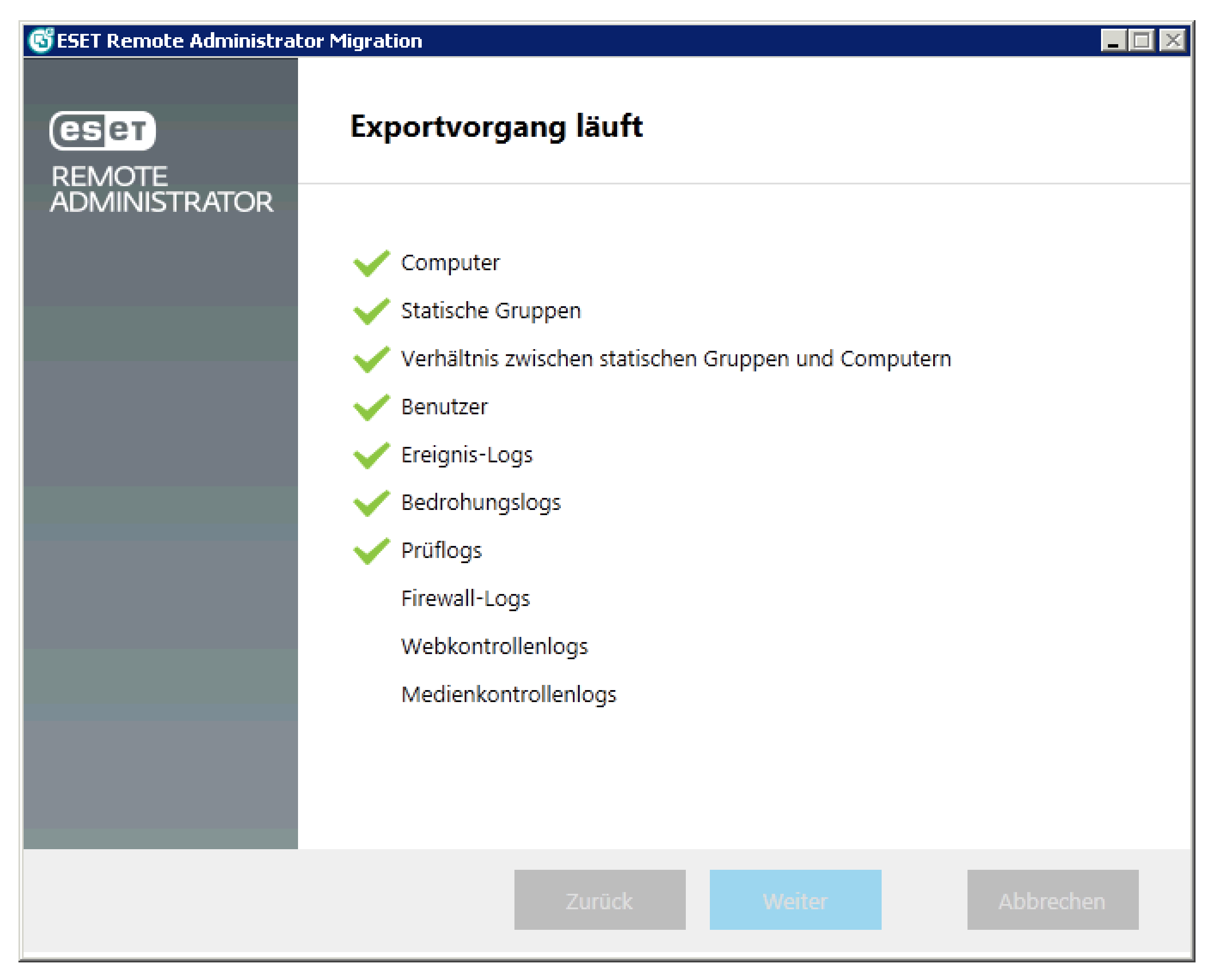
1. Nach dem Ausführen des ESET Remote Administrator-Migrations-Tools auf dem Computer mit ERA 4.x/5.x wählt der Administrator die Option **Exportieren** aus, um die Daten aus ERA 4.x/5.x in einer temporären Datenbankdatei zu speichern. Der Migrationsassistent kann nur bestimmte Daten übertragen.



HINWEIS: Aufgrund des neuen Aufbaus und der neuen Funktionen der dynamischen Gruppen in ERA 6.x können parametrische Gruppen, Tasks und Policies nicht aus ERA 4.x/5.x übertragen werden.



2. Nachdem Sie einen Ordner zum Speichern der temporären Datenbank ausgewählt haben, zeigt der Assistent den Status der Archivierung der ERA 4.x/5.x-Datenbank an.



3. Alle Daten werden in eine **Zwischendatenbank** exportiert.

- Nach dem erfolgreichen **Exportieren** der Daten und vor der **Bereitstellung** von ERA 6.x muss ERA 4.x/5.x **deinstalliert** werden.
- Nach der Installation des neuen ERA 6.x kann die exportierte Datenbank mit dem Migrations-Tool importiert werden. Der Administrator wird zur Auswahl der gespeicherten Datei aufgefordert.
- Wenn die Servereinstellungen das Importieren bestimmter Daten nicht zulassen, können Sie im Migrations-Tool von ESET Remote Administrator wählen, ob Sie die Einstellungen des ERA 6.x-Servers für bestimmte Komponenten ändern möchten.
- Die einzelnen Komponenten werden dann importiert. Für jede Komponente steht ein **Import-(Migrations-) Log** zur Verfügung. Nach dem Importieren zeigt das Migrations-Tool die Ergebnisse des Importprozesses an.
- Wenn Sie Benutzer migriert haben, wurden die Passwörter zurückgesetzt und durch zufällig erstellte Passwörter ersetzt. Diese Passwörter können im `csv` -Format exportiert werden.
- Der Assistent des Migrations-Tools generiert außerdem ein Skript, mit dem die ERA-Agenten auf den Clientcomputern vorkonfiguriert werden können. Das Skript ist eine kleine ausführbare `.bat` -Datei, die an die Clientcomputer verteilt werden kann.
- Es empfiehlt sich, die migrierten Einstellungen und Daten zu überprüfen, um sicherzustellen, dass der Import erfolgreich ausgeführt wurde. Nach der Überprüfung können Sie das Skript zum Bereitstellen des ERA-Agenten auf einer begrenzten Zahl Computer verwenden, um zu überprüfen, ob die Verbindung zum Server richtig hergestellt wird.

- Wenn die Computer dieser Testgruppe erfolgreich eine Verbindung herstellen, können Sie den Agenten auf den verbleibenden Computern bereitstellen (entweder manuell oder mit einem AD-Synchronisierungstask).

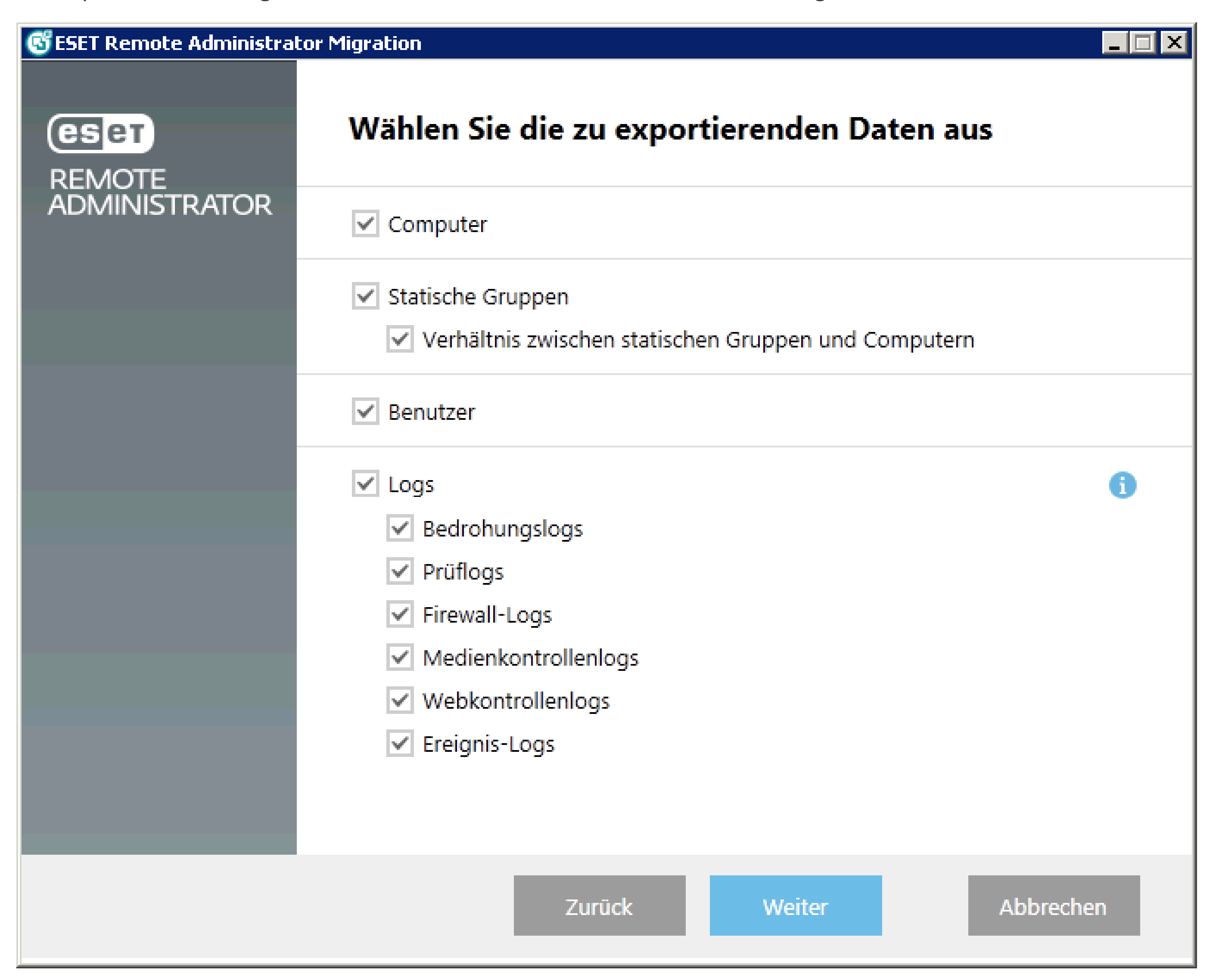
HINWEIS: Wenn bei einem der Migrationsschritte ein Fehler auftritt, machen Sie die für ERA 6.x vorgenommenen Änderungen rückgängig, richten Sie die Computer zur Verbindung mit ERA 4.x/5.x ein, stellen Sie die Sicherungsdaten von ERA 4.x/5.x wieder her und wenden Sie sich an den ESET-Support.

3.10.3 Migrationsszenario 3

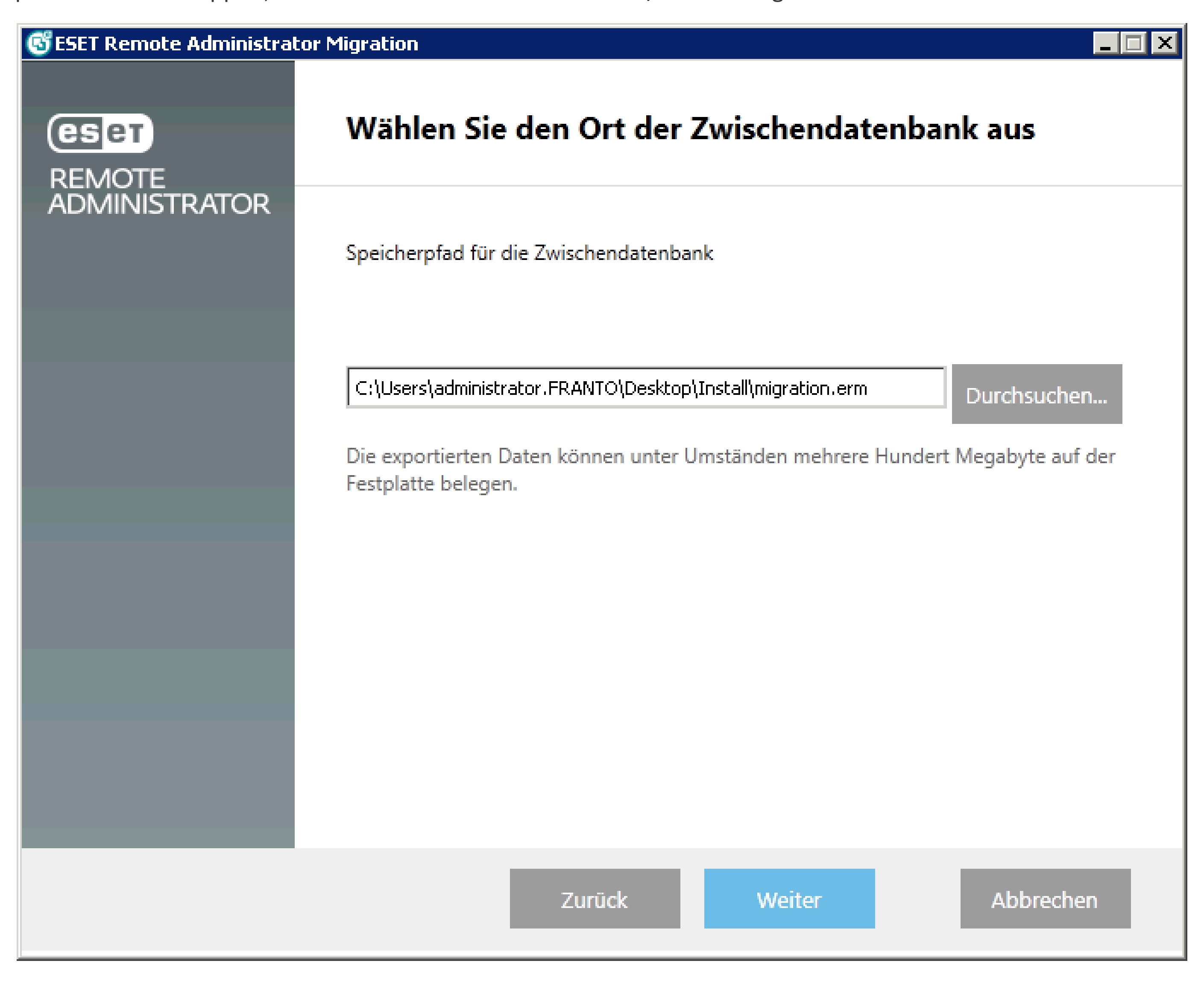
Dieses Szenario gilt für eine Migration auf ERA 6.x, bei der die Endgeräte bis zur Bereitstellung des ERA-Agenten durch ERA 6.x eine Verbindung zum alten ERA 4.x/5.x herstellen.

HINWEIS: Eine Migration in diesem Szenario sollte nur von Experten ausgeführt werden. Diese Art der Migration wird nur empfohlen, wenn keine andere Möglichkeit zur Auswahl steht.

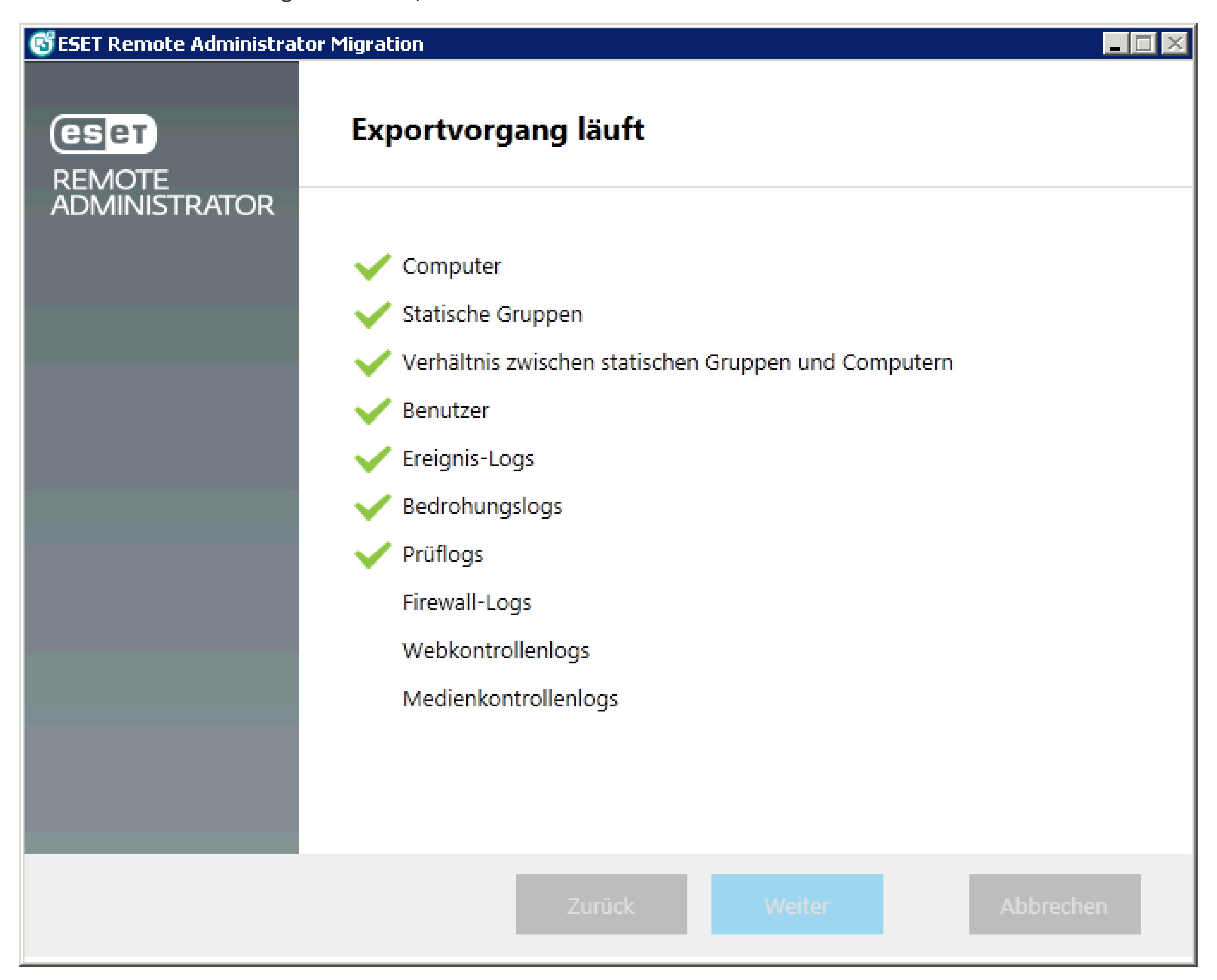
1. Nach dem Ausführen des ESET Remote Administrator-Migrations-Tools auf dem Computer mit ERA 4.x/5.x wählt der Administrator die Option **Exportieren** aus, um die Daten aus ERA 4.x/5.x in einer temporären Datenbankdatei zu speichern. Der Migrationsassistent kann nur bestimmte Daten übertragen.



HINWEIS: Aufgrund des neuen Aufbaus und der neuen Funktionen der dynamischen Gruppen in ERA 6.x können parametrische Gruppen, Tasks und Policies nicht aus ERA 4.x/5.x übertragen werden.



2. Nachdem Sie einen Ordner zum Speichern der temporären Datenbank ausgewählt haben, zeigt der Assistent den Status der Archivierung der ERA 4.x/5.x-Datenbank an.



3. Alle Daten werden in eine **Zwischendatenbank** exportiert.

4. Wenn das neue ERA 6 auf dem gleichen Computer wie 4.x / 5.x installiert werden soll, können Sie die Ports des alten ERA ändern und den Serverdienst umbenennen (`sc config ERA_SERVER DisplayName= "ESET Remote Administrator g1"`).

5. ESET Remote Administrator 4.x / 5.x sollte nach dem Exportieren der Daten neu gestartet werden.

6. Installieren Sie ESET Remote Administrator 6 und importieren Sie die vorübergehende Datenbank mit dem Migrations-Tool.

   - Wenn die Servereinstellungen das Importieren bestimmter Daten nicht zulassen, können Sie im Migrations-Tool von ESET Remote Administrator wählen, ob Sie die Einstellungen des ERA 6.x-Servers für bestimmte Komponenten ändern möchten.

   - Die einzelnen Komponenten werden dann importiert. Für jede Komponente steht ein **Import-(Migrations-) Log** zur Verfügung. Nach dem Importieren zeigt das Migrations-Tool die Ergebnisse des Importprozesses an.

   - Wenn Sie Benutzer migriert haben, wurden die Passwörter zurückgesetzt und durch zufällig erstellte Passwörter ersetzt. Diese Passwörter können im `csv` -Format exportiert werden.

   - Der Assistent des Migrations-Tools generiert außerdem ein Skript, mit dem die ERA-Agenten auf den Clientcomputern vorkonfiguriert werden können. Das Skript ist eine kleine ausführbare `.bat` -Datei, die an die Clientcomputer verteilt werden kann.

- Es empfiehlt sich, die migrierten Einstellungen und Daten zu überprüfen, um sicherzustellen, dass der Import erfolgreich ausgeführt wurde. Nach der Überprüfung können Sie das Skript zum Bereitstellen des ERA-Agenten auf einer begrenzten Zahl Computer verwenden, um zu überprüfen, ob die Verbindung zum Server richtig hergestellt wird.
- Wenn die Computer dieser Testgruppe erfolgreich eine Verbindung herstellen, können Sie den Agenten auf den verbleibenden Computern bereitstellen (entweder manuell oder mit einem AD-Synchronisierungstask).

HINWEIS: Wenn bei einem der Migrationsschritte ein Fehler auftritt, machen Sie die für ERA 6.x vorgenommenen Änderungen rückgängig, richten Sie die Computer zur Verbindung mit ERA 4.x/5.x ein, stellen Sie die Sicherungsdaten von ERA 4.x/5.x wieder her und wenden Sie sich an den ESET-Support.

Bei dieser Art der Migration werden zwischen dem Sichern der ERA 4.x/5.x-Datenbank und dem Bereitstellen des Agenten auf dem Clientcomputer keine Logs exportiert. Diese Daten bleiben jedoch weiterhin im alten Exemplar von ERA 4.x/5.x vorhanden.

4. Erste Schritte

Nachdem Sie ESET Remote Administrator erfolgreich installiert haben, können Sie mit der Einrichtung fortfahren. Die folgenden Kapitel beschreiben die empfohlenen ersten Schritte nach der Installation von ESET Remote Administrator.

Öffnen Sie zunächst die ERA-Web-Konsole in einem Webbrowser und melden Sie sich an.

Erste Schritte mit der ERA-Web-Konsole

Vor der eigentlichen Einrichtung empfehlen wir, den Abschnitt erste Schritte mit der ERA-Web-Konsole zu lesen, da diese Benutzeroberfläche zur Verwaltung der ESET-Sicherheitslösungen verwendet wird.

Hinzufügen von Clientcomputern, Server und Mobilgeräten im Netzwerk zur ERA-Struktur
Während der Installation können Sie das Netzwerk nach Computern (Clients) durchsuchen. Die gefundenen Clients werden im Abschnitt „Computer" aufgelistet, wenn Sie ESET Remote Administrator starten. Wenn im Abschnitt „Computer" keine Clients angezeigt werden, führen Sie den Task Synchronisieren statischer Gruppen aus, um nach Computern zu suchen und sie in Gruppen anzuzeigen.

Bereitstellen eines Agenten
Wenn Computer gefunden wurden, können Sie auf den Clients einen Agenten bereitstellen. Der Agent wird für die Kommunikation zwischen ESET Remote Administrator und den Clients eingesetzt.

Installieren eines ESET-Produkts (einschließlich Aktivierung)
Installieren Sie ESET-Produkte, um die Clients und das Netzwerk zu schützen. Dies können Sie über den Task Software-Installation ausführen.

Erstellen/Bearbeiten von Gruppen
Wir empfehlen, Clients nach verschiedenen Kriterien in statischen oder dynamischen Gruppen anzuordnen. Dies erleichtert die Verwaltung der Clients und hilft Ihnen, einen Überblick über das Netzwerk zu bewahren.

Erstellen einer neuen Policy
Policies sind sehr nützlich, wenn Sie eine bestimmte Konfiguration eines ESET-Produkts, wie sie auf einem Clientcomputer ausgeführt wird, verteilen möchten. So können Sie die Konfiguration über eine Policy erzwingen, statt das ESET-Produkt manuell auf jedem Client konfigurieren zu müssen. Nachdem Sie eine neue Policy mit der benutzerdefinierten Konfiguration erstellt haben, können Sie sie einer (statischen oder dynamischen) Gruppe zuweisen. Die Policy wird daraufhin auf alle Computer der Gruppe angewendet.

Zuweisen einer Policy zu einer Gruppe
Wie oben beschrieben muss eine Policy zum Anwenden einer Gruppe zugewiesen werden. Die Policy wird auf alle Computer angewendet, die in der Gruppe enthalten sind. Die Anwendung der Policy erfolgt bei jeder Verbindung des Agenten zum ERA-Server.

Einrichten von Benachrichtigungen und Erstellen von Berichten
Verwenden Sie Benachrichtigungen und Berichte, um einen besseren Überblick über die Clientcomputer in Ihrer Umgebung zu bewahren. Sie können beispielsweise Benachrichtigungen konfigurieren, die beim Eintreten eines bestimmten Ereignisses ausgelöst werden, oder Berichte anzeigen und herunterladen.

4.1 Öffnen der ERA Web-Konsole

Die ERA Web-Konsole kann auf verschiedene Arten geöffnet werden:

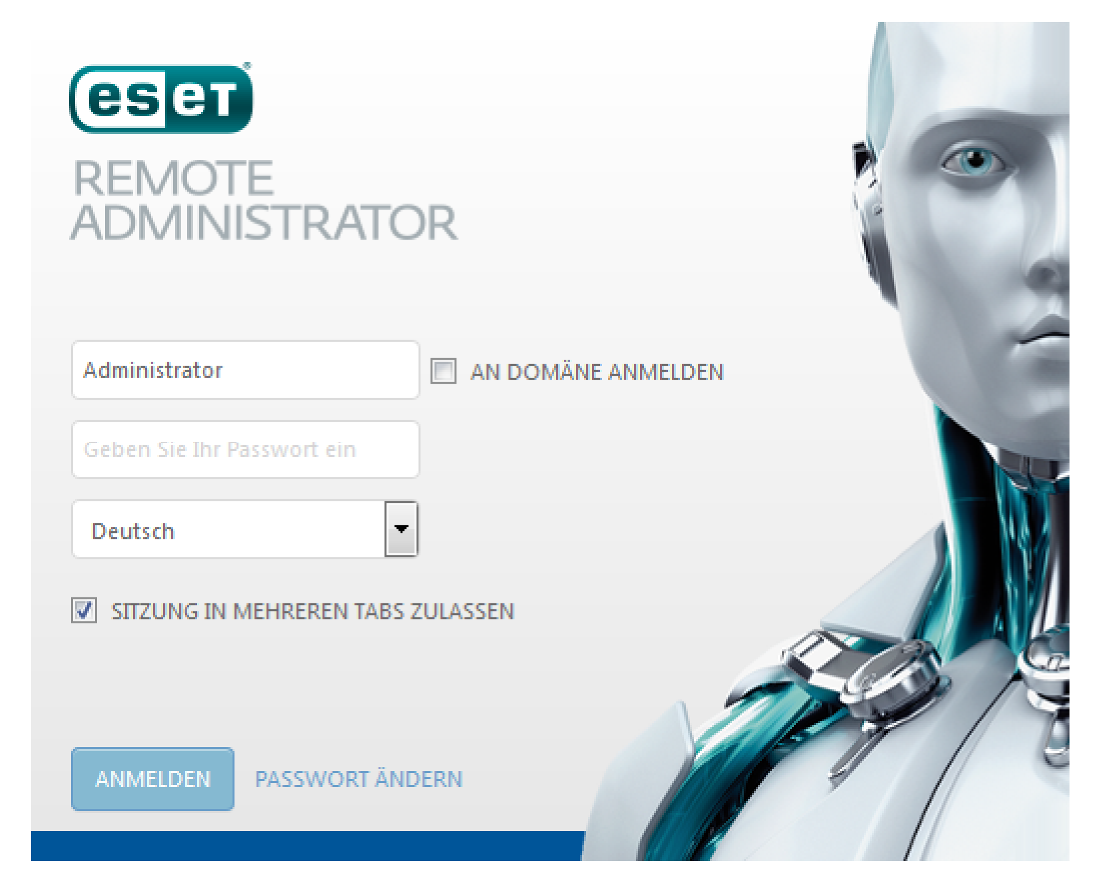
- Geben Sie auf dem lokalen Server (Computer, der als Host für die Web-Konsole fungiert) die folgende URL in einen Webbrowser ein:
  https://localhost/era/

- Geben Sie von anderen, beliebigen Standorten mit Internetzugriff auf den Webserver die URL im folgenden Format ein:
  https://servername/era/
  Ersetzen Sie „servername" mit dem tatsächlichen Namen bzw. der IP-Adresse des Webservers.

- Um sich bei der virtuellen ERA-Appliance anzumelden, verwenden Sie folgende URL:
  https://[IP-Adresse]:8443/
  Ersetzen Sie „[IP-Adresse]“ durch die IP-Adresse der virtuellen ERA-Maschine. Wenn Sie sich nicht mehr an die IP-Adresse erinnern können, siehe Schritt 9 der Bereitstellungsanweisungen für die virtuelle Appliance.
- Klicken Sie auf dem lokalen Server (Maschine, die als Host für die Web-Konsole fungiert), auf Start > **Alle Programme** > **ESET** > **ESET Remote Administrator** > **ESET Remote Administrator-Web-Konsole**. Der Anmeldebildschirm wird in Ihrem Standard-Webbrowser geöffnet. Dies gilt nicht für die virtuelle ERA-Appliance.

HINWEIS: Die Web-Konsole arbeitet mit HTTPS. Daher wird im Webbrowser möglicherweise eine Meldung zu einem Sicherheitszertifikat oder zu einer nicht vertrauenswürdigen Verbindung angezeigt. Der genaue Wortlaut der Meldung hängt vom verwendeten Browser ab. Diese Meldung wird angezeigt, weil der Browser Sie dazu auffordert, die Identität der Website zu bestätigen, auf die Sie zugreifen möchten. Klicken Sie auf **Laden dieser Website fortsetzen** (Internet Explorer) bzw. **Ich kenne das Risiko** und dann auf **Ausnahme hinzufügen...** Klicken Sie dann auf **Sicherheitsausnahme bestätigen** (Firefox), um den Zugriff auf die ERA Web-Konsole zuzulassen. Dies gilt nur, wenn Sie auf die URL der ESET Remote Administrator-Web-Konsole zugreifen.

Wenn der Webserver (auf dem die ERA-Web-Konsole ausgeführt wird) ausgeführt wird, wird der unten abgebildete Bildschirm angezeigt.

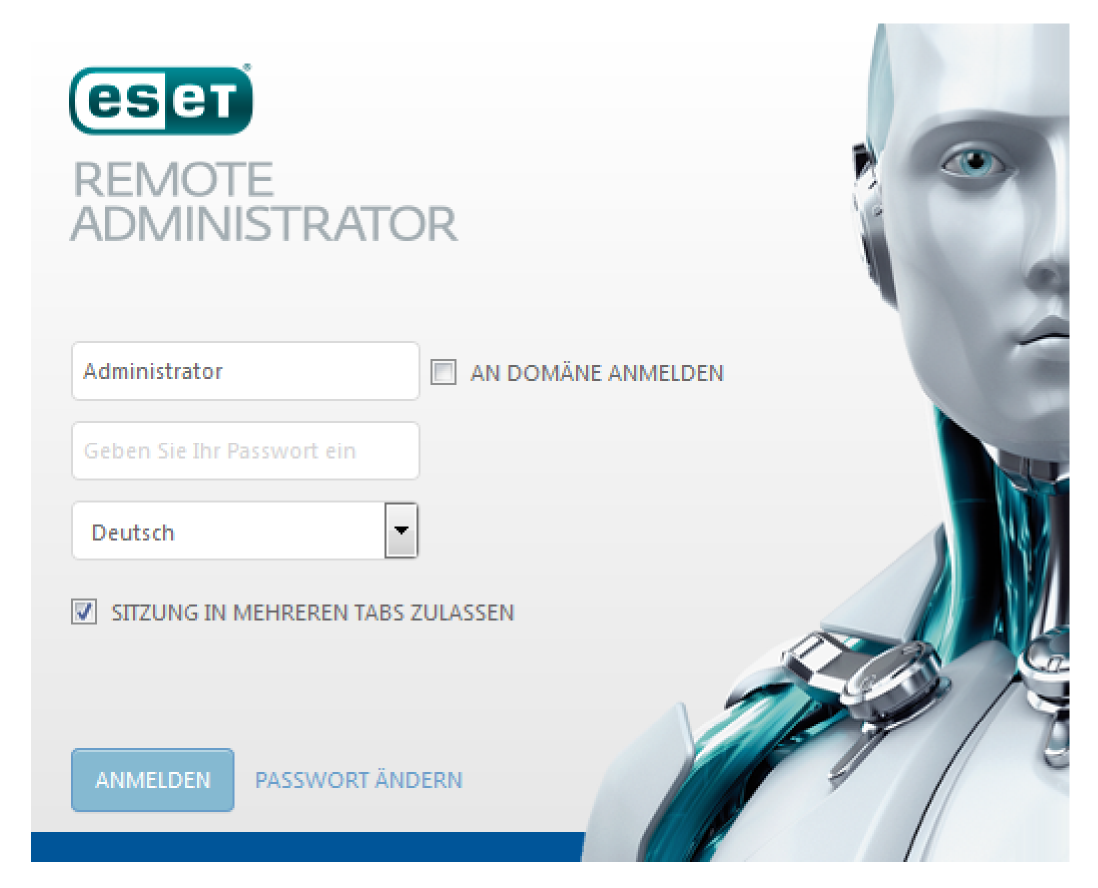


Wenn dies Ihre erste Anmeldung ist, geben Sie die Anmeldedaten ein, die Sie während des Installationsvorgangs eingegeben haben. Weitere Informationen zu diesem Bildschirm finden Sie unter Anmeldebildschirm der Web-Konsole.

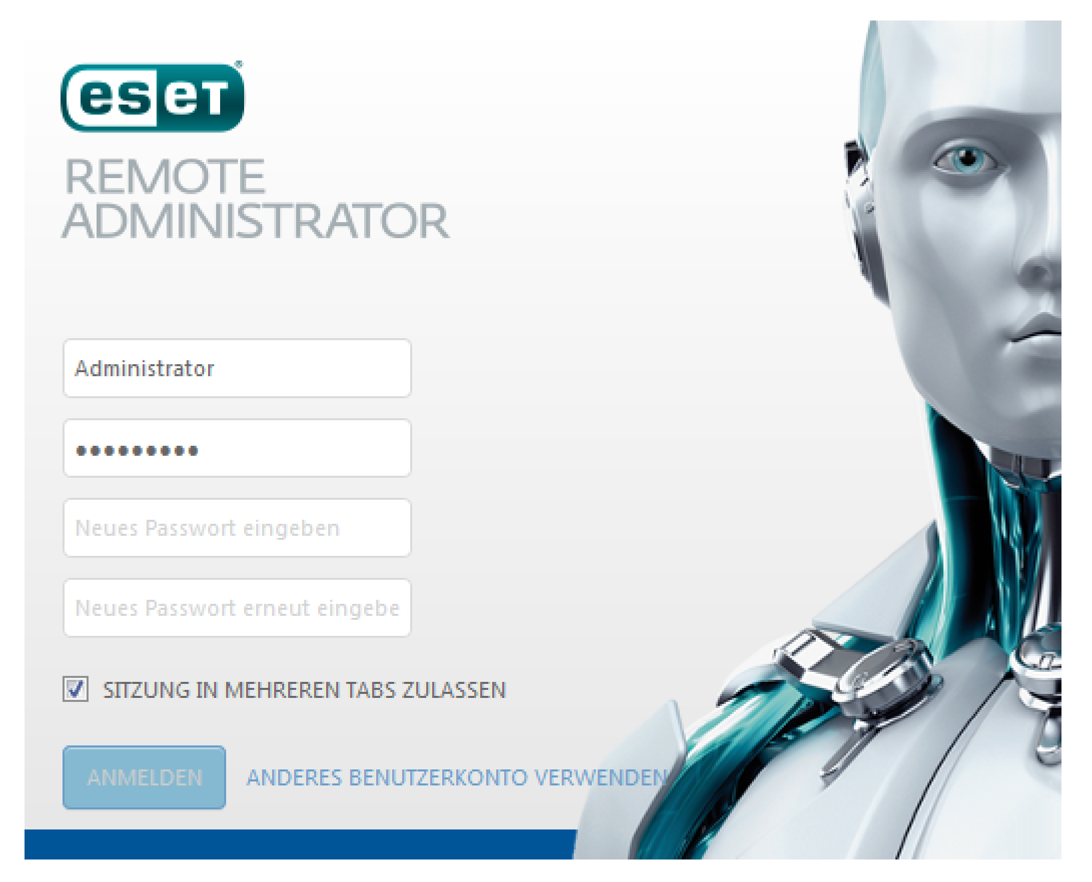
HINWEIS: Sollte der Anmeldebildschirm nicht angezeigt oder dauerhaft neu geladen werden, starten Sie den *ESET Remote Administrator Server*-Dienst neu. Wenn der *ESET Remote Administrator Server*-Dienst wieder ausgeführt wird, starten Sie den *Apache Tomcat*-Dienst neu. Anschließend sollte der Anmeldebildschirm der Web-Konsole erfolgreich geladen werden.

4.2 Anmeldebildschirm der ERA Web-Konsole

Zur Anmeldung bei der Web-Konsole sind Anmeldedaten (Benutzername und Passwort) erforderlich. Sie können sich auch als Domänenbenutzer anmelden. Dazu muss das Kontrollkästchen neben **An Domäne anmelden** aktiviert werden (ein Domänenbenutzer ist nicht mit einer der zugeordneten Domänengruppen verknüpft). Oben rechts im Anmeldebildschirm können Sie aus einer Liste die gewünschte Sprache für die Benutzeroberfläche auswählen. Wählen Sie **Sitzung in mehreren Tabs zulassen** aus, um zuzulassen, dass die Benutzer die ERA-Web-Konsole in mehreren Registerkarten im Browser öffnen.



Passwort ändern/Probieren Sie ein anderes Benutzerkonto: Hier können Sie Ihr Passwort ändern oder zum Anmeldebildschirm zurückkehren. Benutzer ohne Berechtigungssatz können sich an der Web-Konsole anmelden, jedoch keine relevanten Informationen anzeigen.



Die Berechtigungen zum Lesen/Schreiben/Ändern in den Modulen der Web-Konsole werden über Berechtigungssätze erteilt, die erstellt und dem Benutzer zugewiesen werden müssen.

Sitzungsverwaltung und Sicherheitsmaßnahmen:

- **Sperre bei erfolglosen Versuchen von gleicher IP-Adresse**
  Nach 10 erfolglosen Anmeldeversuchen von der gleichen IP-Adresse werden weitere Anmeldeversuche von dieser IP-Adresse ungefähr 10 Minuten lang vorübergehend gesperrt. Die Anmeldesperre auf Grundlage der IP-Adresse beeinflusst keine bestehenden Sitzungen.

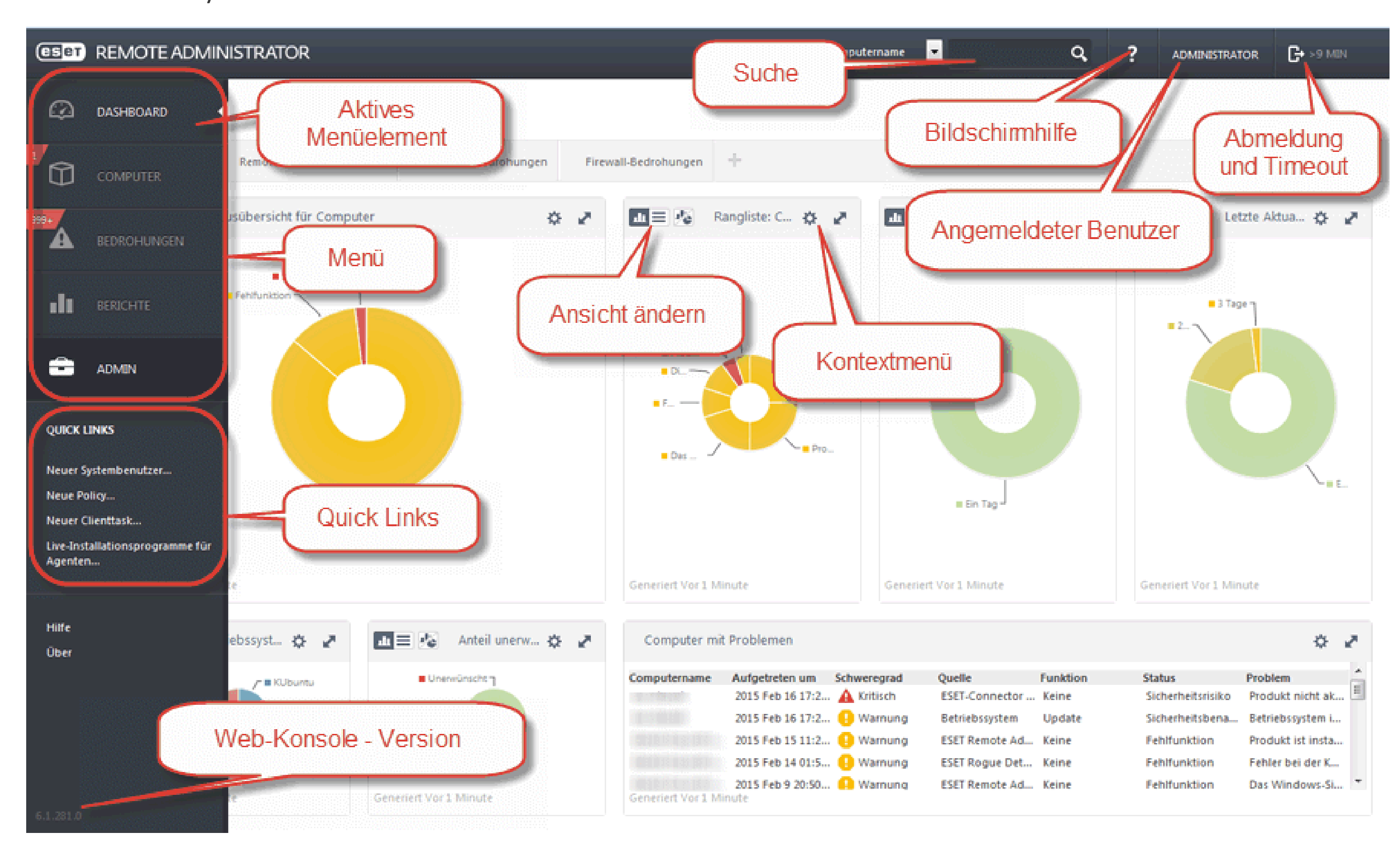
- **Sperre bei Verwendung falscher Sitzungs-ID**
  Wenn von der gleichen IP-Adresse 15 Mal hintereinander eine ungültige Sitzungs-ID verwendet wird, werden alle weiteren Verbindungen von dieser IP-Adresse ungefähr 15 Minuten lang gesperrt. Abgelaufene Sitzungs-IDs werden nicht berücksichtigt. Eine abgelaufene Sitzungs-ID im Browser wird nicht als Angriff eingestuft. Die 15 Minuten dauernde Sperre der IP-Adresse gilt für alle Aktionen (auch gültige Anforderungen).

4.3 Erste Schritte mit der ERA-Web-Konsole

Die Web-Konsole von ESET Remote Administrator ist die primäre Benutzeroberfläche für den ERA-Server. Sie können sich die Web-Konsole als eine Art Systemsteuerung vorstellen, von der aus Sie alle ESET-Sicherheitslösungen verwalten können. Die Web-Konsole ist eine webbasierte Benutzeroberfläche. Der Zugriff erfolgt über einen Browser (siehe Unterstützte Browser) von einem beliebigen Standort aus und mit einem beliebigen Gerät mit Internetzugriff.

Hier finden Sie einige grundlegende Informationen zur Orientierung in der Benutzeroberfläche:

- Der aktuell angemeldete Benutzer wird stets in der oberen rechten Ecke und mit einem Rückwärtszähler für die Gültigkeitsdauer der aktuellen Sitzung angezeigt. Sie können jederzeit neben dem Rückwärtszähler auf **Abmelden** klicken, um sich abzumelden. Wenn die Sitzung aufgrund einer Zeitüberschreitung durch Inaktivität beendet wird, muss sich der Benutzer neu anmelden.
- Sie können in jedem beliebigen Bildschirm oben auf **„?“** klicken, um die **Bildschirmhilfe** für den betroffenen Bildschirm anzuzeigen.
- Das **Menü** ist immer links verfügbar, außer während der Verwendung eines Assistenten. Bewegen Sie zu einem beliebigen Zeitpunkt den Mauszeiger in den linken Bildschirmbereich, um das Menü anzuzeigen. Das Menü enthält außerdem **Quick Links** und zeigt die Version der **Web-Konsole an.**
- Das Zahnradsymbol kennzeichnet ein Kontextmenü.

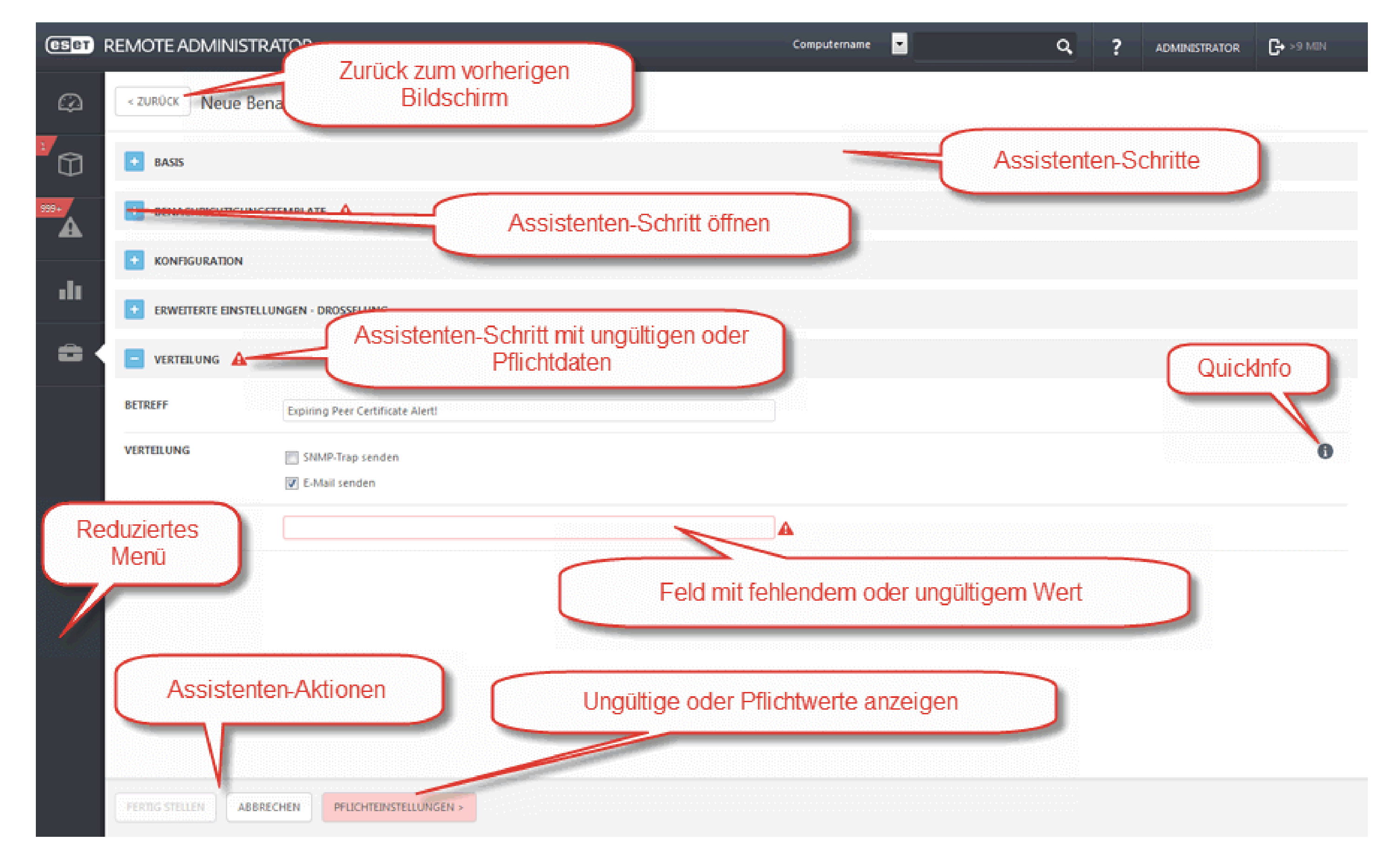


In Bildschirmen mit Baumstruktur sind besondere Steuerelemente verfügbar. Der Baum wird links angezeigt, die Aktionen unten. Klicken Sie im Baum auf ein Element, um die Optionen für dieses Element anzuzeigen.

In Tabellen können Sie Elemente aus Zeilen einzeln oder gruppenweise (bei Auswahl mehrerer Zeilen) verwalten. Klicken Sie auf eine Zeile, um Optionen für die Zeilenelemente anzuzeigen. Die Daten in den Tabellen können gefiltert und sortiert werden.

Die Objekte in ERA können mit Assistenten bearbeitet werden. Die Assistenten weisen einige Gemeinsamkeiten auf:

- Die Schritte sind vertikal von oben nach unten angeordnet.
- Der Benutzer kann jederzeit zu einem beliebigen Schritt zurückkehren.
- Ungültige Eingabedaten werden hervorgehoben, wenn Sie den Cursor in das nächste Feld bewegen. Der Schritt mit ungültiger Dateneingabe wird im Assistent ebenfalls markiert.
- Durch Klicken auf **„Pflichteinstellungen"** kann jederzeit auf ungültige Daten geprüft werden.
- „Fertig stellen" ist erst verfügbar, wenn alle Eingabedaten korrekt sind.



4.4 Bereitstellung

Nach der erfolgreichen Installation von ESET Remote Administrator müssen der **ERA-Agent** und **der ESET-Endpunktschutz (EES, EEA...)** auf den Computern im Netzwerk bereitgestellt werden. Die Bereitstellung umfasst die folgenden Schritte:

1. Clientcomputer zur ESET Remote Administrator-Gruppenstruktur hinzufügen.
2. Bereitstellung des ERA-Agenten
3. Bereitstellung des ESET-Endpunktschutzes

Nach der Bereitstellung des ERA-Agenten können Sie Remote-Installationen anderer ESET-Sicherheitsprodukte auf den Clientcomputern ausführen. Die einzelnen Schritte der Remote-Installation sind im Kapitel Produktinstallation beschrieben.

4.4.1 Hinzufügen eines Clientcomputers zur ERA-Struktur

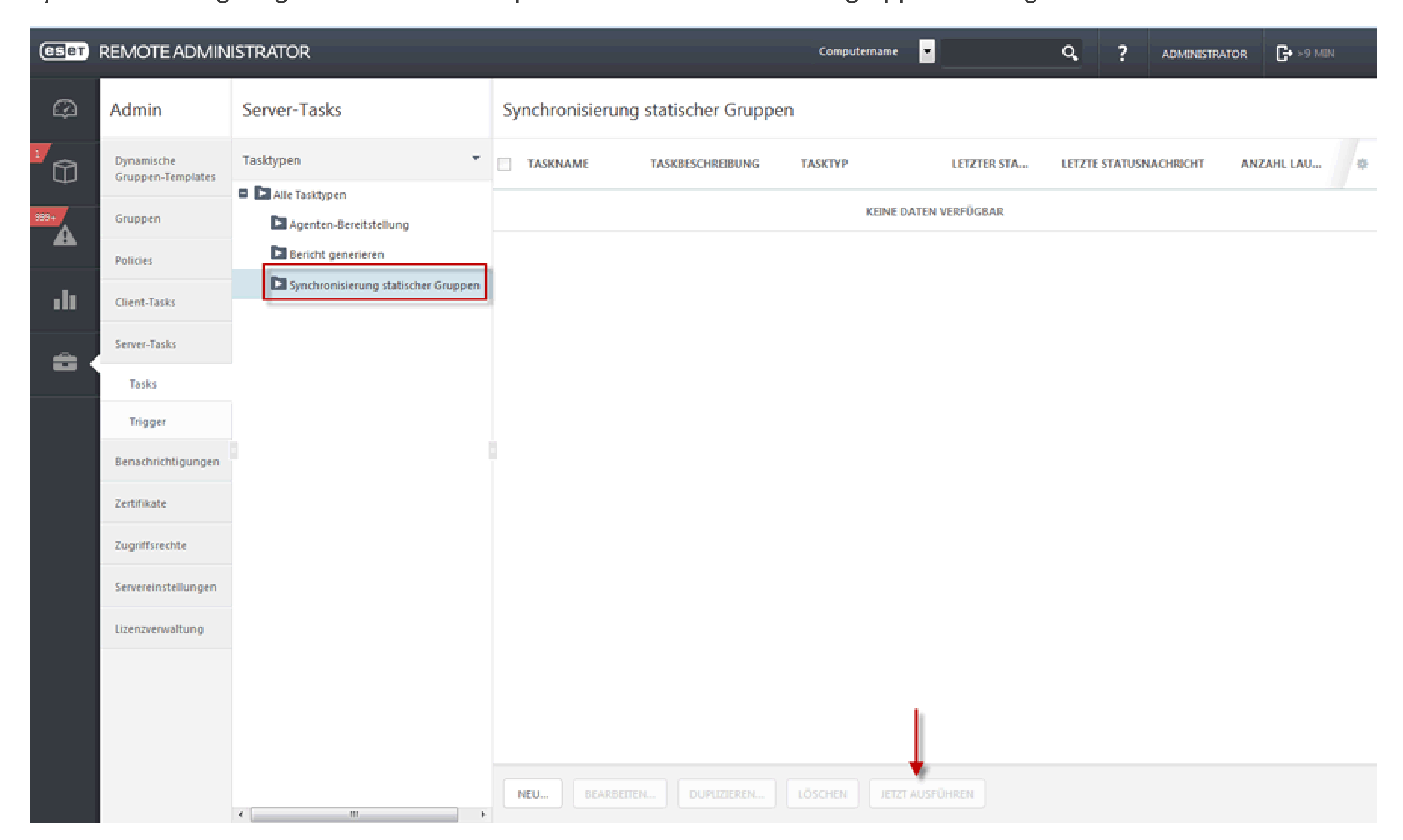
Computer können auf 3 verschiedene Weisen zu ESET Remote Administrator hinzugefügt werden:

- Active Directory-Synchronisierung
- Manuelle Eingabe eines Namens/einer IP-Adresse
- Rogue Detection Sensor

4.4.1.1 Active Directory-Synchronisierung

Die AD-Synchronisierung wird über den Servertask **Synchronisierung statischer Gruppen** ausgeführt.

Admin > **Servertask** ist ein vordefinierter Standardtask, den Sie während der Installation von ESET Remote Administrator automatisch ausführen lassen können. Wenn sich der Computer in einer Domäne befindet, wird die Synchronisierung ausgeführt und die Computer aus AD in der Standardgruppe **Alle** aufgelistet.



Klicken Sie auf den Task und wählen Sie **Jetzt ausführen** aus, um den Synchronisierungsvorgang zu starten. Wenn Sie einen neuen AD-Synchronisierungstask erstellen möchten, wählen Sie eine Gruppe aus, zu der Sie neue Computer aus AD hinzufügen möchten. Wählen Sie die Objekte im AD aus, von denen Sie synchronisieren möchten, und wählen Sie Aktionen für Duplikate aus. Geben Sie die Verbindungseinstellungen für den AD-Server ein und legen Sie den **Synchronisierungsmodus** auf **Active Directory/Open Directory/LDAP** fest.

Weitere Informationen finden Sie in diesem ESET Knowledgebase-Artikel.

4.4.1.2 Manuelle Eingabe eines Namens/einer IP-Adresse

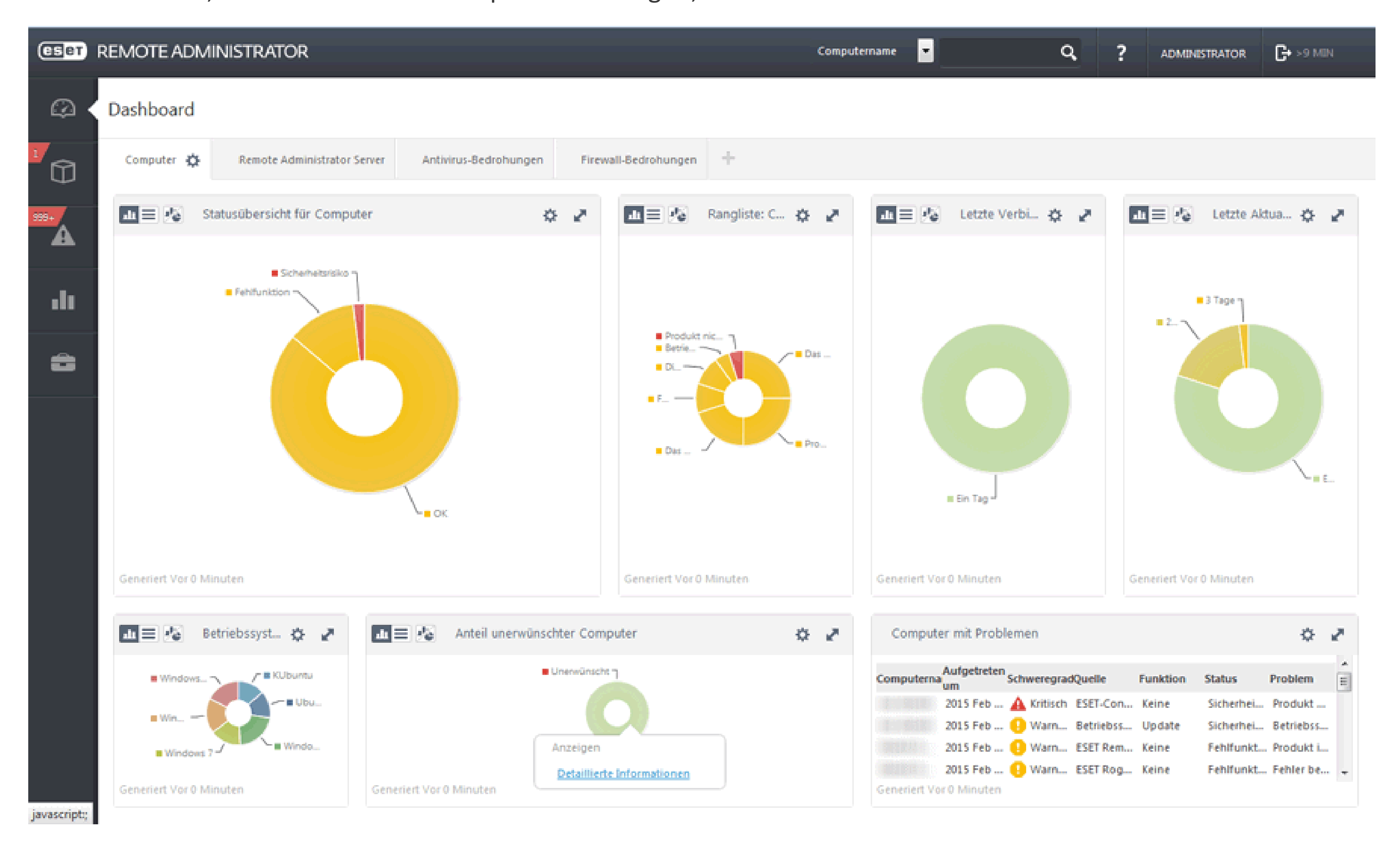
Auf der Registerkarte **Computer** können Sie über die Option **Hinzufügen neue** Computer hinzufügen. Auf diese Weise können Sie Computer hinzufügen, die nicht automatisch gefunden und hinzugefügt wurden.

Geben Sie die **IP-Adresse** oder den **Hostnamen** des Computers ein, den Sie hinzufügen möchten. ESET Remote Administrator führt im Netzwerk eine Suche nach dem Computer aus.

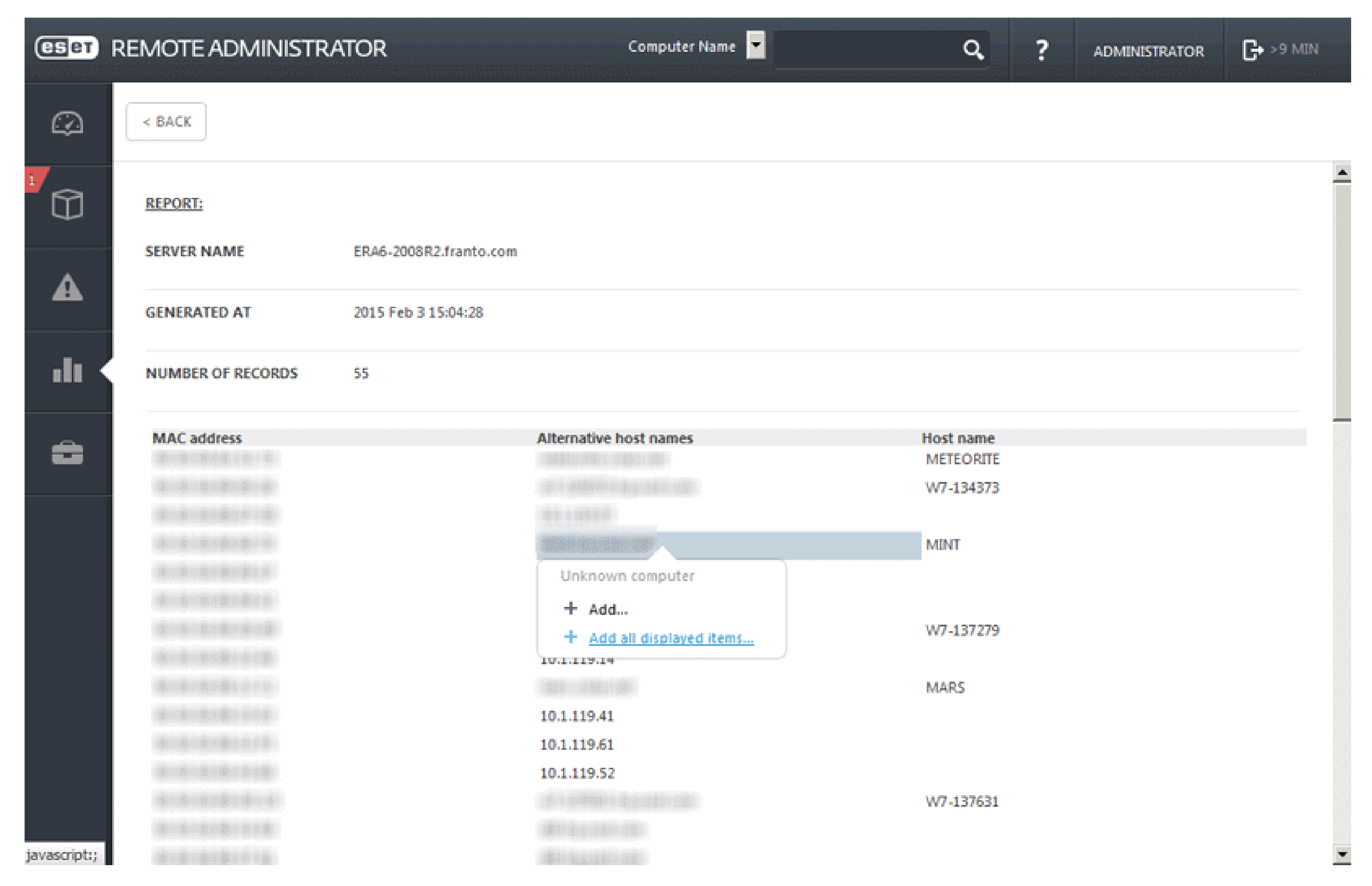
Klicken Sie auf **Hinzufügen**. Wenn Sie eine Gruppe auswählen, werden rechts in der Liste die zur Gruppe gehörenden Computer angezeigt. Nach dem Hinzufügen des Computers wird ein Popup-Fenster mit der Option **Agent bereitstellen** angezeigt.

4.4.1.3 Rogue Detection Sensor

Wenn Sie keine AD-Synchronisierung verwenden, ist die einfachste Lösung zum Hinzufügen eines Computers in die ERA-Struktur die Verwendung von **RD Sensor**. Die RD Sensor-Komponente ist Bestandteil des Installationspakets. Führen Sie einen Drilldown im Bericht **Anteil unerwünschter Computer** im unteren Bereich des Computer-Dashboards aus, um unerwünschte Computer anzuzeigen, indem Sie auf den roten Teil der Grafik klicken.

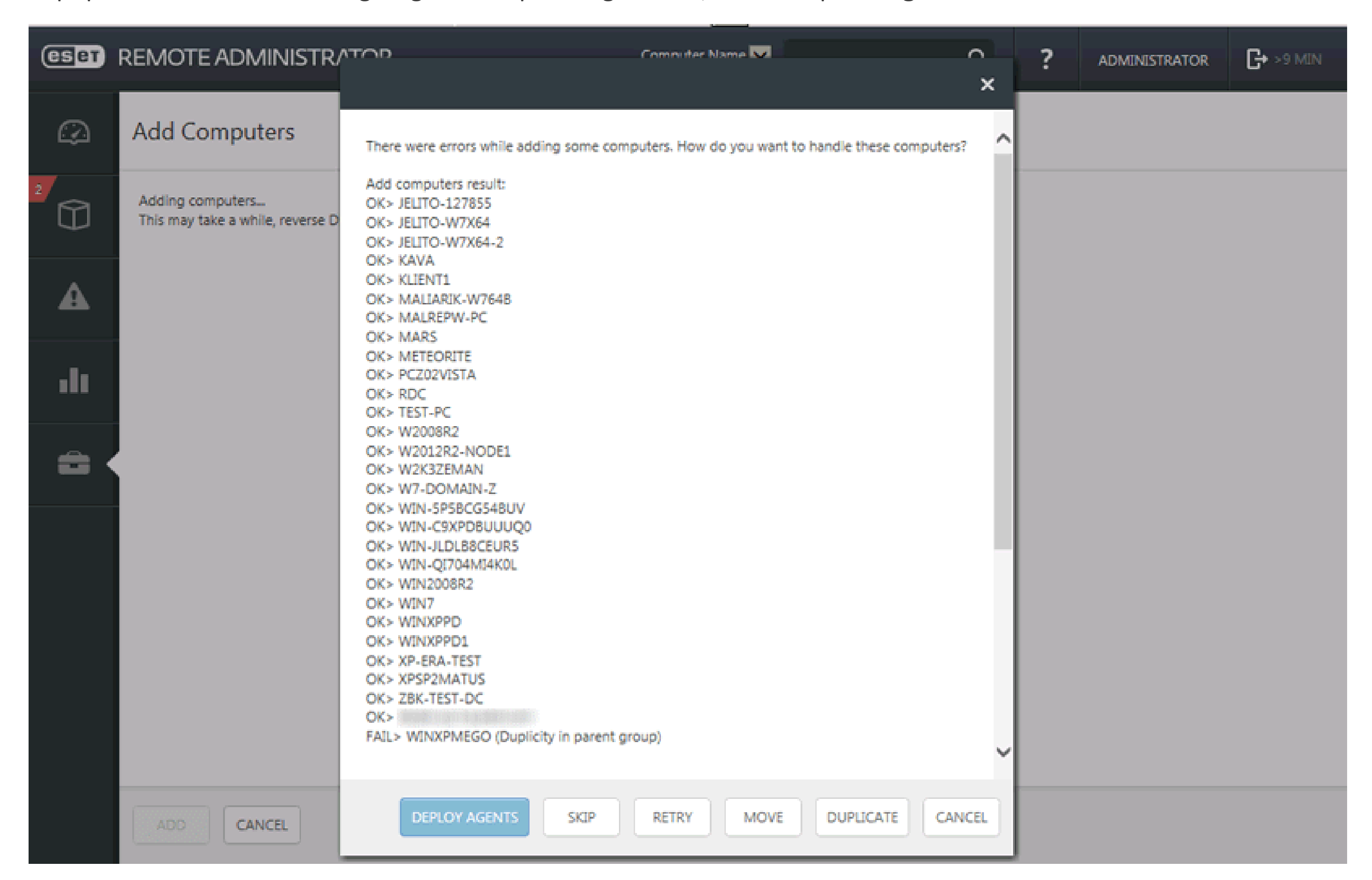


Im Bericht **Unerwünschte Computer** im Dashboard werden nun die vom RD Sensor erfassten Computer angezeigt. Um einen ausgewählten Computer hinzuzufügen, klicken Sie auf den gewünschten Computer und dann auf **Hinzufügen**. Alternativ können Sie Alle angezeigten Elemente hinzufügen.



Befolgen Sie die Anweisungen auf dem Bildschirm, wenn Sie einen einzelnen Computer hinzufügen möchten. Sie können einen vordefinierten Namen verwenden oder einen eigenen Namen angeben. Der Name ist nur ein Anzeigename, der in der ERA-Web-Konsole angezeigt wird, nicht ein Hostname. Geben Sie wahlweise eine Beschreibung ein. Wenn der Computer bereits im ERA-Verzeichnis vorhanden ist, werden Sie darüber informiert und können auswählen, wie mit dem Duplikat vorgegangen werden soll. Folgende Optionen stehen zur Verfügung: **Agent bereitstellen**, **Überspringen**, **Wiederholen**, **Verschieben**, **Duplizieren** und **Abbrechen**. Nach dem Hinzufügen des Computers wird ein Popup-Fenster mit der Option **Agent bereitstellen** angezeigt.

Wenn Sie **Alle angezeigten Elemente hinzufügen** auswählen, wird eine Liste der hinzuzufügenden Computer angezeigt. Klicken Sie neben dem Namen eines Computers auf „X“, wenn der Computer momentan nicht in das ERA-Verzeichnis aufgenommen werden soll. Wenn Sie keine Computer mehr aus der Liste entfernen möchten, klicken Sie auf **Hinzufügen**. Wählen Sie dann aus, welche Aktion ausgeführt werden soll, wenn ein Duplikat gefunden wird (je nach Anzahl der Computer in der Liste kann eine kurze Verzögerung auftreten): **Überspringen**, **Wiederholen**, **Verschieben**, **Duplizieren** und **Abbrechen**. Nachdem Sie eine Option ausgewählt haben, wird ein Popup-Fenster mit den hinzugefügten Computern geöffnet, das die Option **Agent bereitstellen** enthält.



Die Ergebnisse des RD-Sensor-Scans werden in die Log-Datei `detectedMachines.log` geschrieben. Die Datei enthält eine Liste der im Netzwerk erkannten Computer. Die Datei `detectedMachines.log` befindet sich in folgendem Verzeichnis:

- Windows
  C:\ProgramData\ESET\Rouge Detection Sensor\Logs
- Linux
  var/log/eset/RemoteAdministrator/RogueDetectionSensor/detectedMachines.log

4.4.2 Agenten-Bereitstellung

Die Agenten-Bereitstellung kann auf verschiedene Weisen erfolgen. Folgende Bereitstellungsmethoden stehen zur Verfügung:

Remote - über einen Servertask für die Massenbereitstellung des ERA-Agenten. Alternativ können Sie den Agenten mithilfe von GPO und SCCM bereitstellen
Lokal - mithilfe des Agenten-Installationspakets oder Live-Installationsprogramms für Agenten, zum Beispiel wenn bei der Remote-Bereitstellung Probleme auftreten

Die lokale Bereitstellung kann auf drei verschiedene Weisen ausgeführt werden:

- Live-Installationsprogramm für Agenten - Unter Verwendung eines generierten Skripts in der ERA Web-Konsole können Sie das Live-Installationsprogramm für Agenten per E-Mail verteilen oder von einem Wechselmedium (z. B. einem USB-Speicher) ausführen
- Servergestützte Installation - unter Verwendung des Agenten-Installationspakets. Die Zertifikate werden automatisch vom ERA-Server heruntergeladen (empfohlen für die lokale Bereitstellung)
- Offline-Installation - mit dem Agenten-Installationspaket. Bei dieser Bereitstellungsmethode müssen Sie die Zertifikate manuell exportieren

Der Task zur Remote-Bereitstellung von Agenten kann zur Massenverteilung von Agenten auf die Clientcomputer verwendet werden. Dies ist die bequemste Verteilungsmethode, da sie von der Web-Konsole aus ausgeführt werden kann und der Agent nicht manuell auf jedem Computer einzeln bereitgestellt werden muss.

Der ERA-Agent ist eine wichtige Komponente, weil die Kommunikation zwischen den ESET-Sicherheitslösungen auf den Clientcomputern und dem ERA-Server ausschließlich über den Agenten erfolgt.

HINWEIS: Wenn bei der Remote-Bereitstellung des ERA-Agenten Probleme auftreten (d. h. der Servertask **Agenten-Bereitstellung** schlägt fehl), beachten Sie die Hinweise unter Fehlerbehebung.

4.4.2.1 Bereitstellungsschritte – Windows

1. Vergewissern Sie sich, dass alle **Voraussetzungen** erfüllt sind:

- **Der ERA-Server** und die **ERA Web-Konsole** sind installiert (auf einem Servercomputer).
- Ein Agenten-Zertifikat wurde erstellt und auf dem lokalen Laufwerk vorbereitet.
- Eine Zertifizierungsstelle ist auf dem lokalen Laufwerk vorbereitet.
- Der Zugriff auf den **Servercomputer** muss über das Netzwerk möglich sein.

HINWEIS: Wenn bei der Remote-Bereitstellung des ERA-Agenten Probleme auftreten (d. h. der Servertask **Agenten-Bereitstellung** wird mit einem Fehlerstatus beendet), beachten Sie die Hinweise unter Fehlerbehebung.

2. Doppelklicken Sie auf das Installationspaket, um die Installation zu starten.

3. Geben Sie einen **Server-Hostnamen** (Hostname oder IP-Adresse) und einen **Serverport** (standardmäßig 2222) in die entsprechenden Felder ein. Diese Angaben werden für die Verbindung zum ERA-Server verwendet.

4. Wählen Sie ein Peerzertifikat und ein Passwort für das Zertifikat aus. Fügen Sie optional eine Zertifizierungsstelle hinzu. Dies ist nur für nicht signierte Zertifikate erforderlich.

5. Wählen Sie einen Ordner aus, in dem der **Agent** installiert wird, oder lassen Sie den vordefinierten Ordner ausgewählt.

6. Klicken Sie auf **Installieren**. Der **Agent** wird auf dem Computer installiert.

HINWEIS: Wenn Sie einen detaillierten Log der Installation benötigen, starten Sie die Installation über das Programm *msiexec* und geben Sie die erforderlichen Parameter an: `msiexec /i program_installer.msi /lv* c:\temp\installer_log.txt`

- Vergewissern Sie sich, dass der Ordner *c:\temp* vorhanden ist, bevor Sie diesen Befehl ausführen.

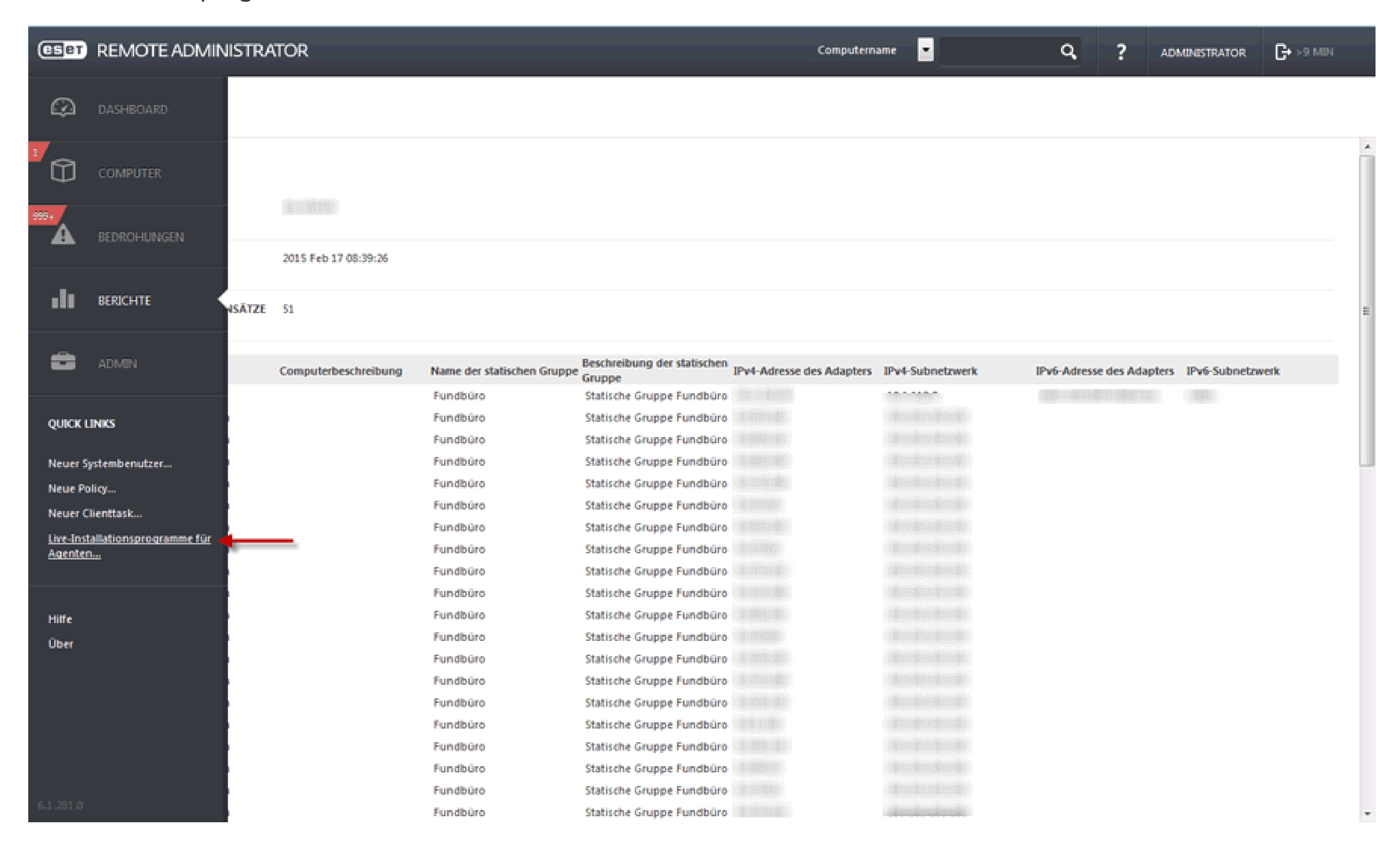
- Im Status-Log auf dem Clientcomputer *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* können Sie überprüfen, ob der ERA-Agent richtig ausgeführt wird.

4.4.2.1.1 Live-Installationsprogramme für Agenten

Diese Art der Agenten-Bereitstellung ist hilfreich, wenn die Optionen zur Remotebereitstellung und zur lokalen Bereitstellung nicht geeignet sind. In diesen Fällen können Sie das Live-Installationsprogramm für den Agenten per E-Mail verschicken und die Bereitstellung durch den Benutzer ausführen lassen. Sie können das Live-Installationsprogramm für den Agenten auch von einem Wechselmedium (z. B. einem USB-Speicher) ausführen.

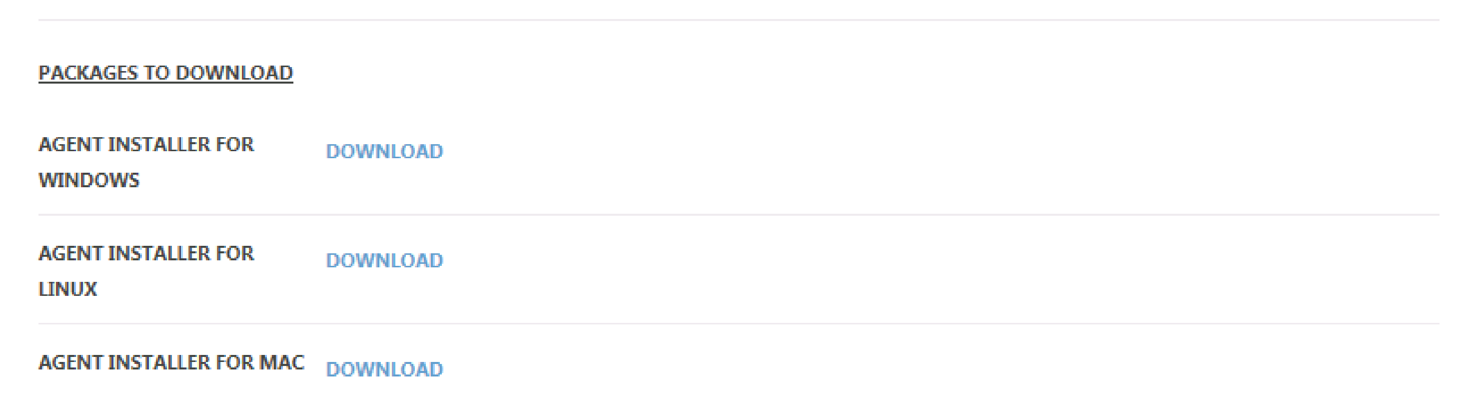
HINWEIS: Auf dem Clientcomputer muss eine Internetverbindung verfügbar sein, um das Agenten-Installationspaket herunterzuladen. Außerdem muss der Client eine Verbindung zum ERA-Server herstellen können.

1. Klicken Sie in den **Quick Links** in der Menüleiste auf **Live-Installationsprogramme für Agenten...**, um das Installationsprogramm zu erstellen.



2. Geben Sie den Hostnamen oder die IP-Adresse des Servers ein und wählen Sie die **ERA-Zertifizierungsstelle** aus, die Sie bei der ursprünglichen Installation erstellt haben. Wenn Sie dazu aufgefordert werden, geben Sie die **Passphrase der Zertifikatsbehörde** ein, die Sie bei der **Serverinstallation** erstellt haben.

3. Klicken Sie auf **Installationsprogramme abrufen**, um Links für die Agenten-Installationsprogramme für Windows, Linux und MAC zu erstellen.



4. Klicken Sie auf den **Download**-Link neben den Installationsprogrammen, die Sie herunterladen möchten, und speichern Sie sie als **ZIP**-Datei. Entzippen Sie die Datei auf dem Clientcomputer, auf dem Sie den ERA-Agenten bereitstellen möchten. Führen Sie auf dem Clientcomputer das Skript `EraAgentOnlineInstaller.bat` (Windows) bzw. `EraAgentOnlineInstaller.sh` (Linux und Mac) aus, um das Installationsprogramm auszuführen.

HINWEIS: Wenn Sie das Skript unter Windows XP SP2 ausführen, müssen Sie das Microsoft Windows Server 2003 Administration Tools Pack installieren. Andernfalls wird das Live-Installationsprogramm für den Agenten nicht richtig ausgeführt. Nachdem Sie das Verwaltungspaket installiert haben, können Sie das Skript des Live-Installationsprogramms für den Agenten ausführen.

Im Status-Log auf dem Clientcomputer *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html* können Sie überprüfen, ob der ERA-Agent richtig ausgeführt wird. Bei Problemen mit dem Agenten (z. B. bei Problemen mit der Verbindung zum ERA-Server) beachten Sie die Hinweise im Abschnitt Fehlerbehebung.

Falls Sie den ERA-Agenten mit dem Live-Installationsprogramm aus Ihrem lokalen freigegebenen Ordner ohne ESET Repository Download-Server bereitstellen möchten, führen Sie die folgenden Schritte aus:

1. Bearbeiten Sie die Skriptdatei `EraAgentOnlineInstaller.bat` (Windows) bzw. `EraAgentOnlineInstaller.sh` (Linux and Mac).
2. Ändern Sie die Zeilen 28 und 30, sodass diese auf die korrekten lokalen Downloaddateien zeigen. Beispiel:

```
27
28 set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x64.msi
29 if defined IsArch_x86 (
30   set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.1.365.0/Agent_x86.msi
31 )
```

3. Verwenden Sie Ihre eigene URL (anstelle der hier gezeigten URL):

```
26 )
27
28 set url=\\server\share\Agent_x64.msi
29 if defined IsArch_x86 (
30   set url=\\server\share\Agent_x86.msi
31 )
```

4. Bearbeiten Sie Zeile 80 und ersetzen Sie " **^& packageLocation ^&** "

```
79 echo.
80 echo.Dim params: params = "/qr /i " ^& packageLocation ^& " /l*v %temp%\ra-agent-install.log" ^&_
```

durch **!url!**

```
79 echo.
80 echo.Dim params: params = "/qr /i !url! /l*v %temp%\ra-agent-install.log" ^&_
```

5. **Speichern** Sie die Datei.

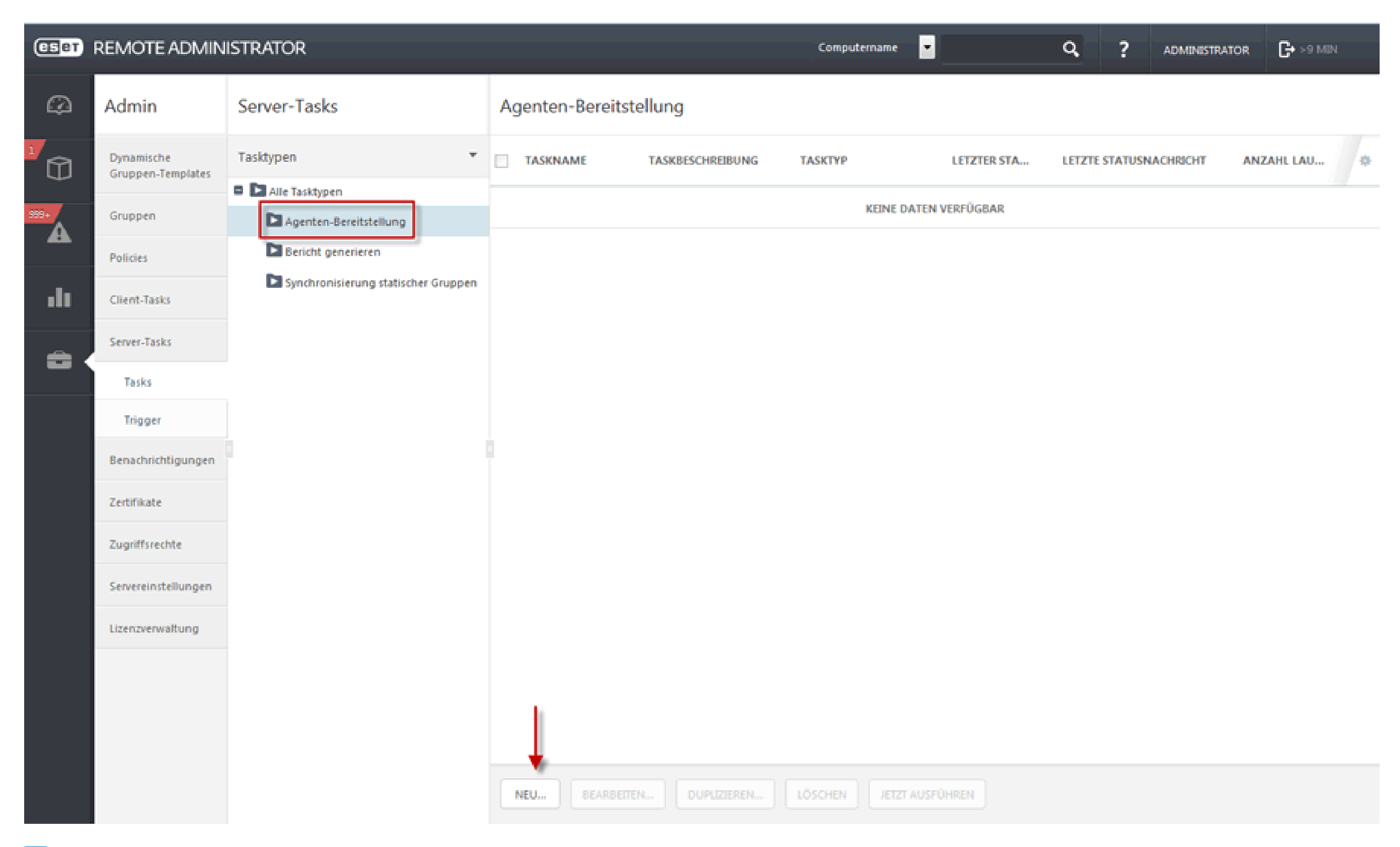
4.4.2.1.2 Remote-Bereitstellung des Agenten

Die Remote-Bereitstellung des ERA-Agenten kann auf zwei verschiedene Arten ausgeführt werden. Sie können einen Servertask wie unten beschrieben verwenden, oder den Agenten mithilfe von GPO und SCCM bereitstellen.

Die Remote-Bereitstellung des ERA-Agenten über einen Servertask wird im Bereich **Admin** ausgeführt. Führen Sie die folgenden Anweisungen aus oder sehen Sie sich das Anleitungsvideo in der Knowledgebase an.

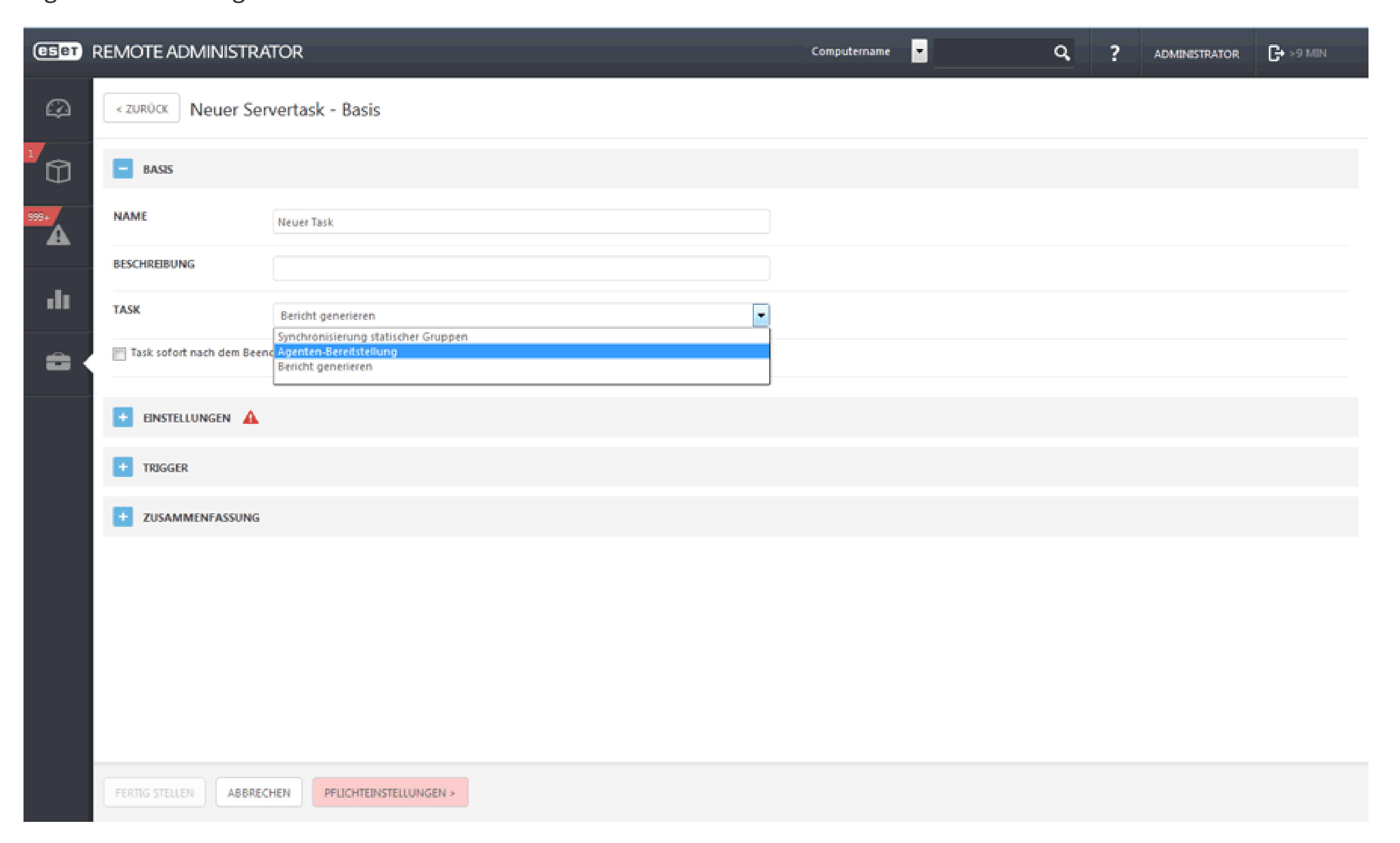
HINWEIS: Sie sollten die massenhafte Agenten-Bereitstellung unbedingt in Ihrer Umgebung testen, bevor Sie den ERA-Agenten auf großen Gruppen von Clients bereitstellen. Setzen Sie das Agenten-Verbindungsintervall nach Ihren Wünschen, bevor Sie die massenhafte Bereitstellung testen.

Klicken Sie auf **Servertask** > **Agenten-Bereitstellung** > **Neu ...**, um mit der Konfiguration des neuen Task zu beginnen.



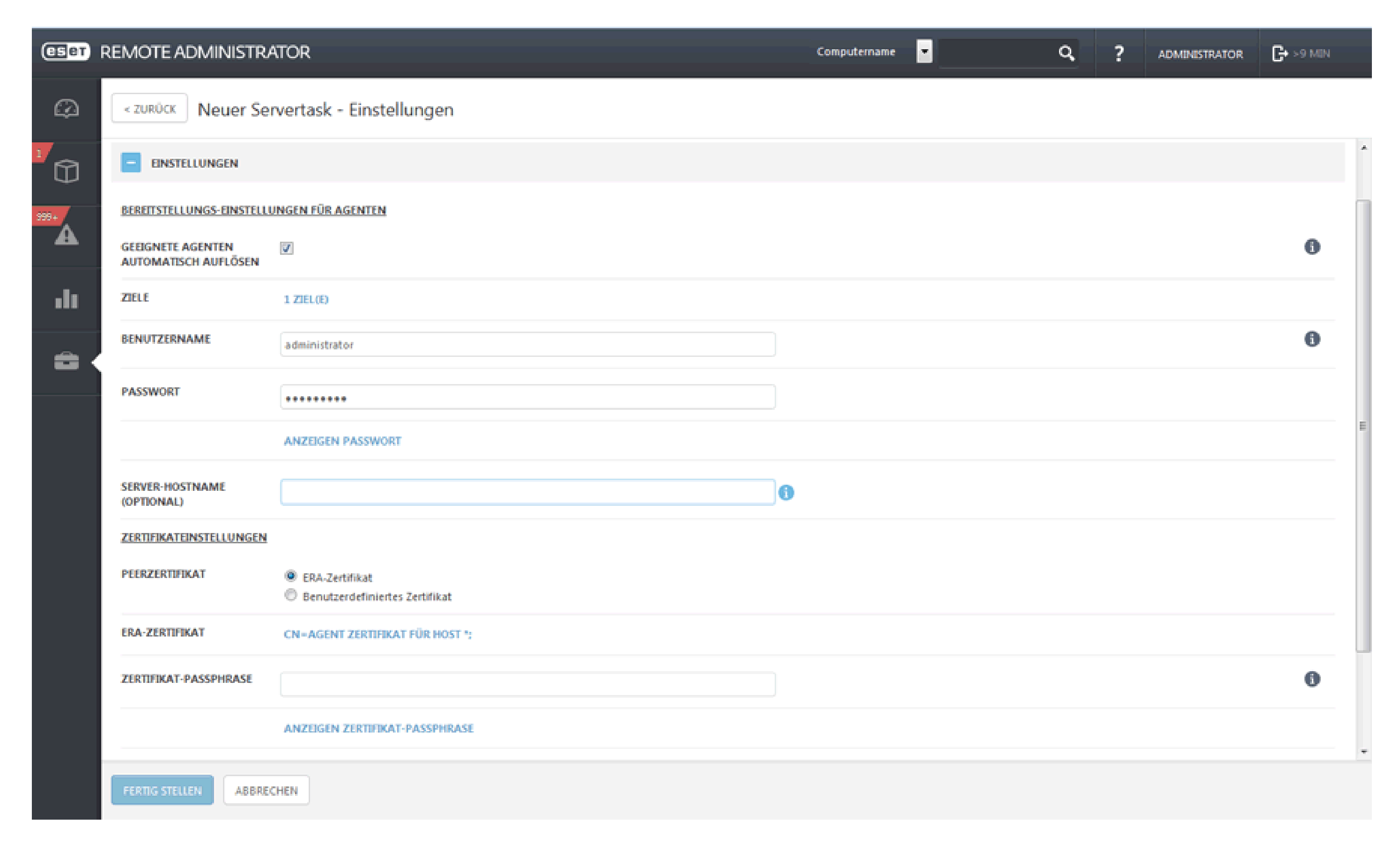
Einfach

Geben Sie grundlegende Informationen zum Task ein, wie **Name**, **Beschreibung** (optional) und **Tasktyp**. Der **Tasktyp** legt die Einstellungen und das Verhalten des Tasks fest.



Einstellungen

- **Geeignete Agenten automatisch auflösen** – Wenn in Ihrem Netzwerk mehrere Betriebssysteme (Windows, Linux, Mac OS) verwendet werden, wählen Sie diese Option aus, damit der Task für jedes System automatisch das geeignete und serverkompatible Agenten-Installationspaket ermittelt.
- **Ziele** – Klicken Sie auf diese Option, um die Clients auszuwählen, die Empfänger des Task sein sollen.
- **Benutzername/Passwort** – Benutzername und Passwort eines Benutzers mit ausreichenden Rechten zum Ausführen einer Remote-Installation des Agenten.
- **Server-Hostname (optional)** – Hier können Sie einen Server-Hostnamen eingeben, falls auf der Clientseite und der Serverseite unterschiedliche Hostnamen verwendet werden.
- **Peerzertifikat/ERA-Zertifikat** – Sicherheitszertifikat und Zertifizierungsstelle für die Agenten-Installation. Sie können das standardmäßige Zertifikat mit Zertifizierungsstelle auswählen oder benutzerdefinierte Zertifikate verwenden. Weitere Informationen finden Sie im Kapitel Zertifikate.
- **Benutzerdefiniertes Zertifikat** – Wenn Sie für die Authentifizierung ein benutzerdefiniertes Zertifikat verwenden, navigieren Sie während der Installation des Agenten zum Zertifikat und wählen Sie es aus.
- **Zertifikat-Passphrase** – Passwort für das Zertifikat: entweder das Passwort, das Sie während der Serverinstallation (beim Erstellen der Zertifizierungsstelle) eingegeben haben, oder das Passwort Ihres benutzerdefinierten Zertifikats.



HINWEIS: Der ERA-Server kann automatisch das geeignete Agenten-Installationspaket für das entsprechende Betriebssystem ermitteln. Um manuell ein Paket zu wählen, deaktivieren Sie **Geeignete Agenten automatisch auflösen** und wählen Sie über das ERA-Repository das gewünschte Paket aus der Liste der verfügbaren Agenten.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.

Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.

Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

HINWEIS: Falls Probleme bei der Remote-Bereitstellung des ERA-Agenten auftreten (der Servertask **Agenten-Bereitstellung** wird mit einem Fehler beendet), beachten Sie die Hinweise im Abschnitt Fehlerbehebung in diesem Handbuch.

4.4.2.1.3 Lokale Bereitstellung des Agenten

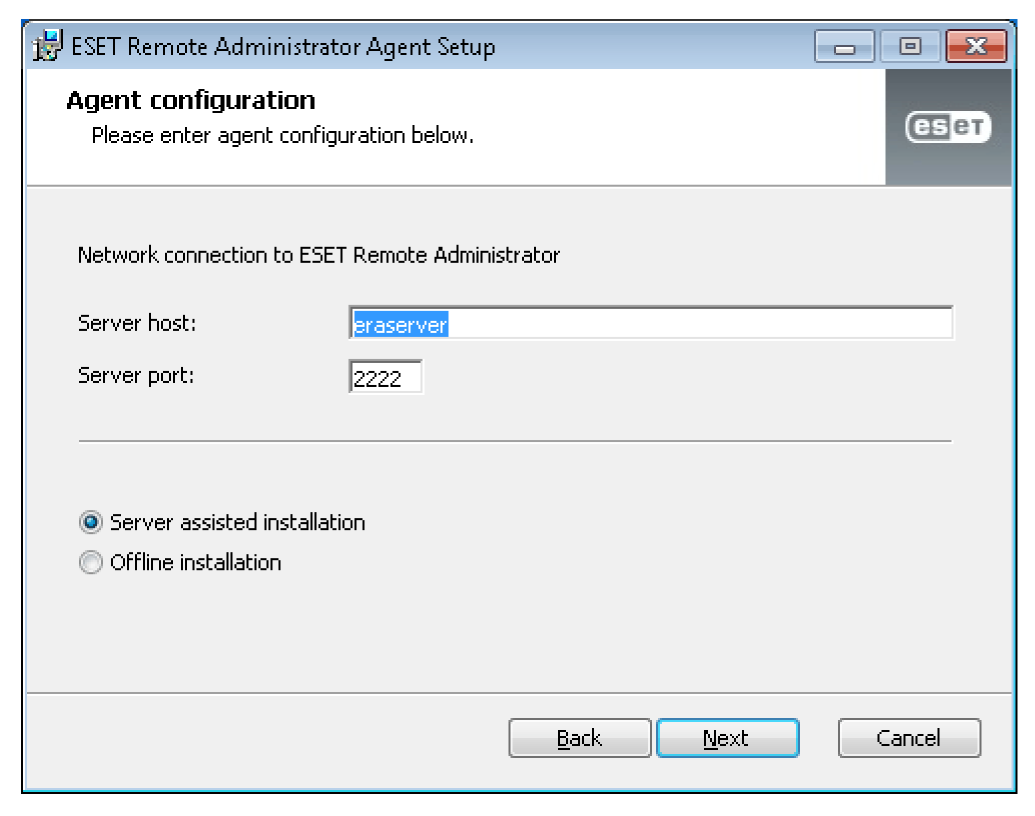
Führen Sie folgende Schritte aus, um den Agenten mit dem Installationsassistenten lokal auf einem Clientcomputer bereitzustellen:

Laden Sie das Agenteninstallationspaket im Downloadbereich der ESET-Website unter **Remote Management** herunter (klicken Sie auf das Symbol „+“, um die Kategorie auszuklappen). Führen Sie das Installationsprogramm auf dem Clientcomputer aus, auf dem der Agent bereitgestellt werden soll. Akzeptieren Sie die EULA und wählen Sie den gewünschten Installationstyp aus: servergestützte Installation oder Offline-Installation.

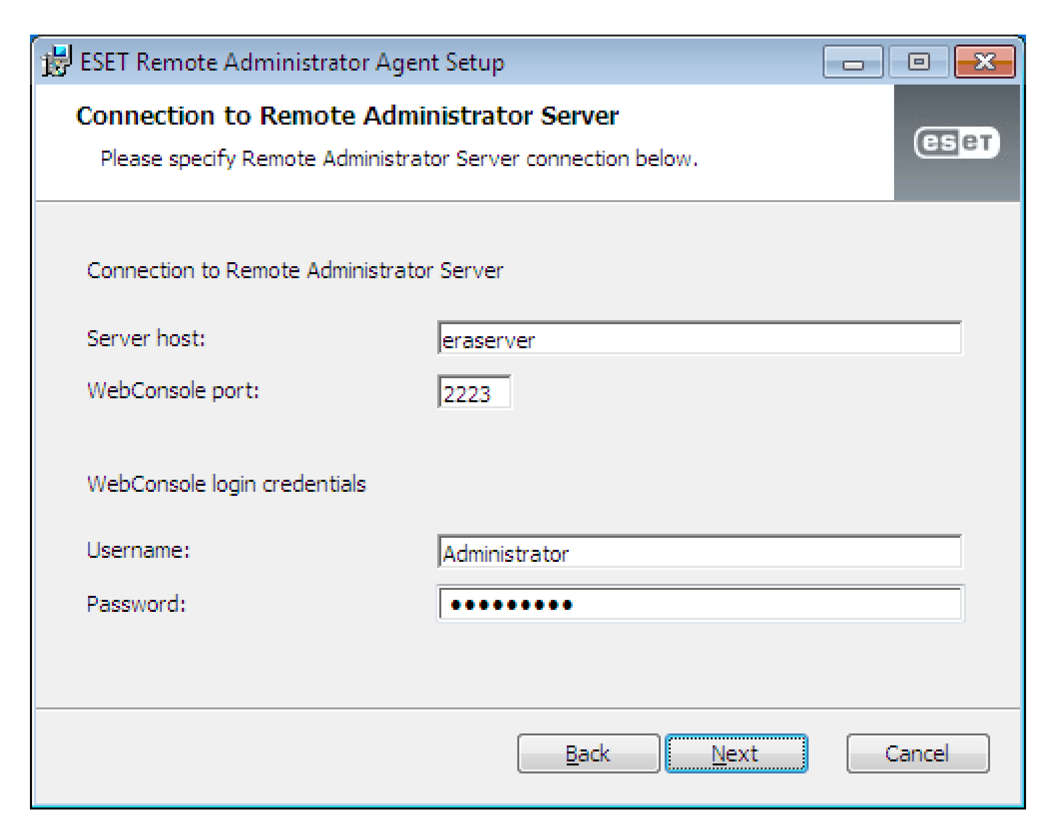
Führen Sie die folgenden Anweisungen aus oder sehen Sie sich das Anleitungsvideo in der Knowledgebase an. In diesem ESET Knowledgebase-Artikel finden Sie außerdem ausführliche Anweisungen.

1. **Servergestützte Installation**:

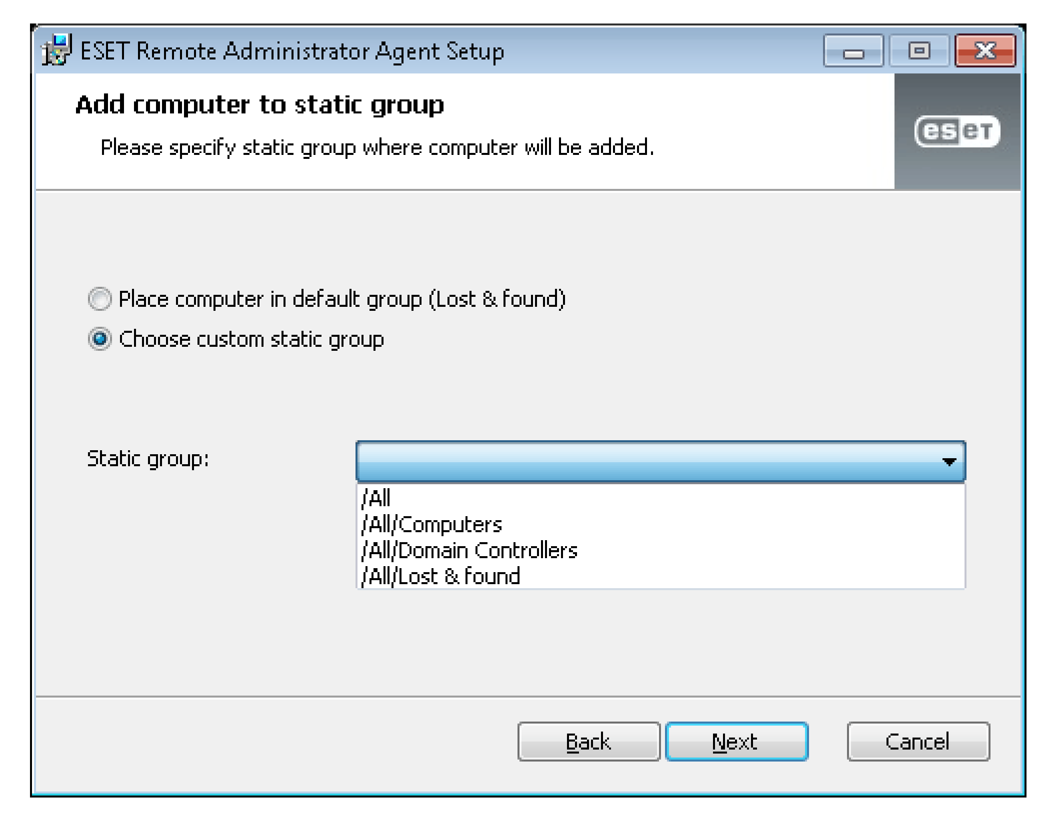
Vergewissern Sie sich, dass **Servergestützte Installation** ausgewählt ist, geben sie den **Serverhost** (Name oder IP-Adresse) und den **Serverport** des ERA-Servers ein und klicken Sie auf **Weiter**. Der standardmäßige Serverport ist 2222. Wenn Sie einen anderen Port verwenden, ersetzen Sie den standardmäßigen Port mit der benutzerdefinierten Portnummer.



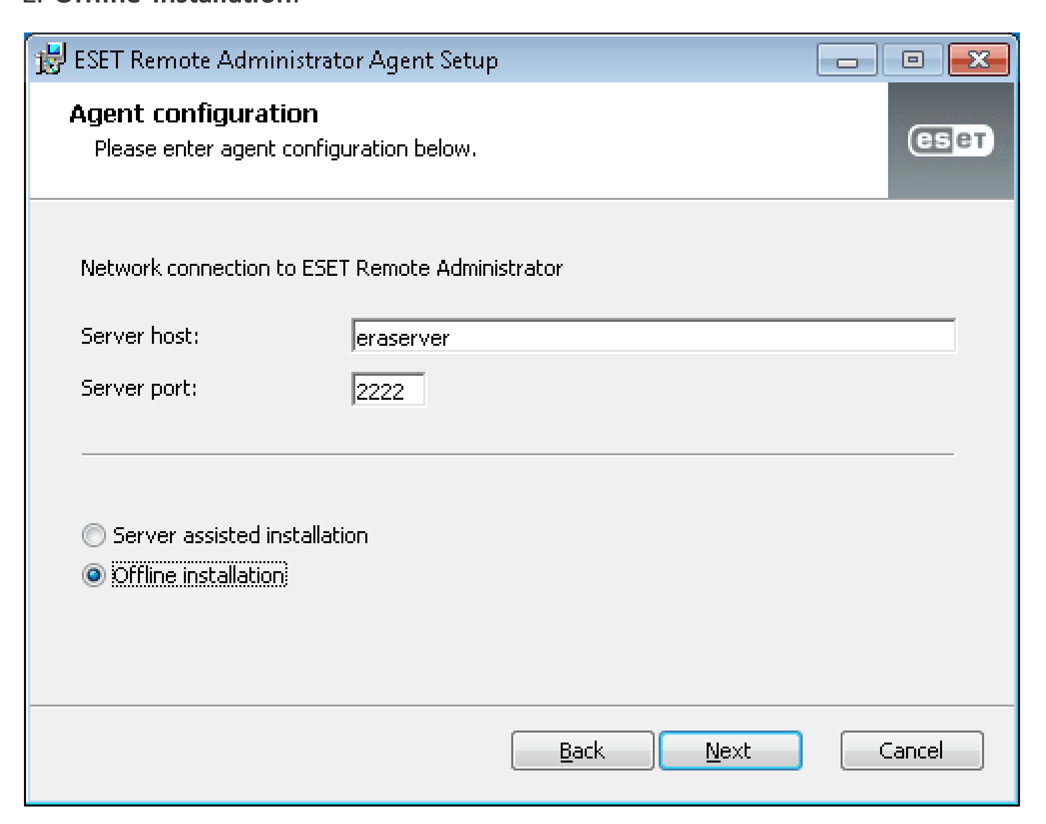
Legen Sie die Methode für die Verbindung zum Remote Administrator Server fest: **ERA-Server** oder **ERA-Proxyserver** und Port der ERA Web-Konsole. Geben Sie die Anmeldedaten für die ERA Web-Konsole ein: **Benutzername** und **Passwort**.



Klicken Sie auf **Benutzerdefinierte statische Gruppe auswählen** und wählen Sie im Dropdownmenü die statische Gruppe aus, zu der der Clientcomputer hinzugefügt werden soll.

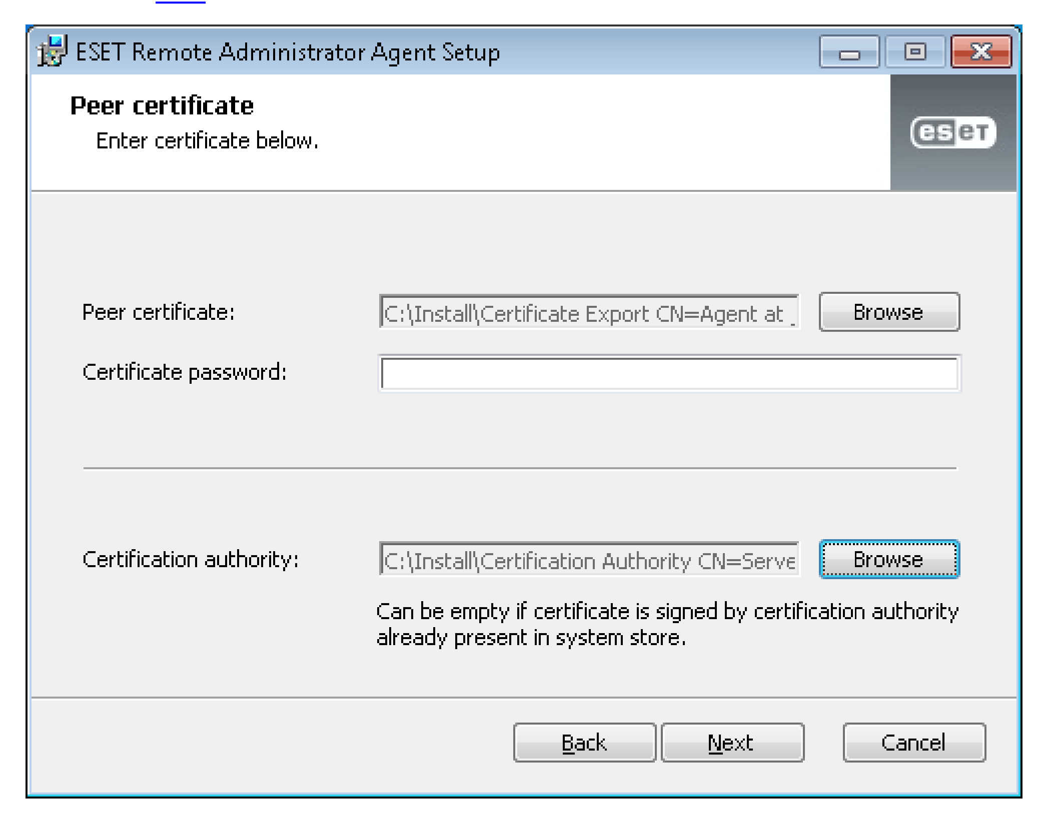


2. **Offline-Installation**:



Wenn Sie die **Offline-Installation** wählen, geben Sie im Feld **Server-Port** den Wert **2222** ein, wählen Sie **Offline-Installation** aus und klicken Sie auf **Weiter**. Bei dieser Methode müssen Sie ein **Peerzertifikat** und eine **Zertifizierungsstelle** angeben.

Weitere Informationen zum Exportieren und Verwenden eines **Peerzertifikats** und einer **Zertifizierungsstelle** finden Sie hier.



HINWEIS: Im Status-Log auf dem Clientcomputer (unter *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html)* können Sie überprüfen, ob der ERA-Agent richtig ausgeführt wird. Bei Problemen mit dem Agenten (z. B. bei Problemen mit der Verbindung zum ERA-Server) beachten Sie die Hinweise im Abschnitt Fehlerbehebung.

4.4.2.2 Bereitstellungsschritte – Linux

Diese Schritte gelten für das Ausführen einer lokalen Installation des Agenten. Wenn Sie den Agenten auf mehreren Computern bereitstellen möchten, lesen Sie den Abschnitt Agenten-Bereitstellung.

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind:

- Der ERA-Server und die ERA Web-Konsole sind installiert (auf einem Servercomputer).
- Ein Agenten-Zertifikat wurde erstellt und auf dem lokalen Laufwerk vorbereitet.
- Eine Zertifizierungsstelle ist auf dem lokalen Laufwerk vorbereitet.
- Der Zugriff auf den **Servercomputer** muss über das Netzwerk möglich sein.
- Die Agenten-Installationsdatei muss als ausführbare Datei (chmod +x) festgelegt sein.

Der Agent wird durch Ausführen eines Befehls im Terminal (siehe Beispiel unten) installiert.

Beispiel
(Neue Zeilen sind mit "\" gekennzeichnet, damit Sie die Zeichenkette leichter zum Terminal kopieren können.)

```
./Agent-Linux-i686-1.0.387.0.sh --skip-license --cert-path=/home/adminko/Desktop/agent.pfx \
--cert-auth-path=/home/adminko/Desktop/CA.der --cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 --port=2222
```

Der ERA-Agent und der eraagent.service werden am folgenden Speicherort installiert:
/opt/eset/RemoteAdministrator/Agent

Installationsparameter

- *--skip-license* verhindert, dass der Benutzer zur Bestätigung der Lizenz aufgefordert wird.
- *--cert-path* ist der Pfad zur Agenten-Zertifikatdatei.
- *--cert-auth-path* ist der Pfad zur Server-Zertifikatsbehördendatei.
- *--cert-password* muss mit dem Passwort des Agenten-Zertifikats übereinstimmen.
- *--hostname* ist eine Verbindung zu einem Server (oder Proxy) in einem dieser Formate (Hostname, IPv4, IPv6 oder SRV-Datensatz).
- *--port* ist ein Port zur Überwachung, sowohl für den Server als auch für den Proxy (2222).

Führen Sie den folgenden Befehl aus, um die ordnungsgemäße Installation zu überprüfen:
```
sudo service eraagent status
```

HINWEIS: Wenn Sie ein Zertifikat verwenden, das Sie erstellt haben und das von einer anderen Zertifizierungsstelle als der ERA-Zertifizierungsstelle signiert wurde, muss der Parameter *--cert-auth-path* im Installationsskript ausgelassen werden, weil die andere Zertifizierungsstelle bereits auf dem Linux-Betriebssystem (und dem Servercomputer) installiert ist.

HINWEIS: Falls Probleme bei der Remote-Bereitstellung des ERA-Agenten auftreten (der Servertask **Agenten-Bereitstellung** wird mit einem Fehlerstatus beendet), beachten Sie die Hinweise im Leitfaden zur Fehlerbehebung.

Im Status-Log auf dem Clientcomputer */var/log/eset/RemoteAdministrator/Agent/trace.log* oder */var/log/eset/RemoteAdministrator/Agent/status.html* können Sie überprüfen, ob der ERA-Agent richtig ausgeführt wird.

4.4.2.3 Bereitstellungsschritte – OS X

1. Vergewissern Sie sich, dass alle **Voraussetzungen** erfüllt sind:

- **Der ERA-Server** und die **ERA Web-Konsole** sind installiert (auf einem Servercomputer).
- Ein Agenten-Zertifikat wurde erstellt und auf dem lokalen Laufwerk vorbereitet.
- Eine Zertifizierungsstelle ist auf dem lokalen Laufwerk vorbereitet.

HINWEIS: Falls Probleme bei der Remote-Bereitstellung des ERA-Agenten auftreten (der Servertask **Agenten-Bereitstellung** wird mit einem Fehlerstatus beendet), beachten Sie die Hinweise im Leitfaden zur Fehlerbehebung.

2. Doppelklicken Sie auf die *DMG*-Datei, um die Installation zu starten.

3. Geben Sie die Informationen für die **Serververbindung** ein: **Server-Hostname** (Hostname/IP-Adresse des ERA-Servers) und **Serverport** (Standardwert: 2222).

4. Wählen Sie ein Peerzertifikat und ein Passwort für das Zertifikat aus. Fügen Sie optional eine Zertifizierungsstelle hinzu. Dies ist nur für nicht signierte Zertifikate erforderlich.

5. Überprüfen Sie das Installationsverzeichnis und klicken Sie auf **Installieren**. Der **Agent** wird auf dem Computer installiert.

6. Die Log-Datei des ERA-Agenten befindet sich unter folgendem Pfad: */Library/Application Support/ com.eset.remoteadministrator.agent/Logs/*

4.4.2.4 Fehlerbehebung – Agenten-Bereitstellung

Möglicherweise treten bei der Agenten-Bereitstellung Fehler auf. Fehler bei der Bereitstellung können verschiedene Ursachen haben. Dieser Abschnitt unterstützt Sie beim

- Ermitteln der Fehlerursache bei der Agenten-Bereitstellung
- Prüfen möglicher Ursachen anhand der nachstehenden Tabelle
- Beheben des Problems und Ausführen einer erfolgreichen Bereitstellung

Windows

1. Um die Ursache des Fehlers bei der Agenten-Bereitstellung zu ermitteln, navigieren Sie zu **Berichte** > **Automatisierung** und wählen Sie **Informationen zu Bereitstellungs-Tasks für Agenten der letzten 30 Tage** aus. Klicken Sie dann auf Jetzt generieren.
Eine Tabelle mit Informationen zur Bereitstellung wird angezeigt. In der Spalte **Fortschritt** werden Fehlermeldungen zur Ursache der fehlgeschlagenen Agenten-Bereitstellung angezeigt.

Wenn Sie zusätzliche Details benötigen, können Sie die im ERA-Server-Log angezeigten Mindestinformationen anpassen. Navigieren Sie hierzu zu **Admin** > **Servereinstellungen** > **Erweiterte Einstellungen** > **Logging** und wählen Sie **Fehler** aus dem Dropdown-Menü aus. Führen Sie die Agenten-Bereitstellung erneut aus. Falls erneut Fehler auftreten, finden Sie unten in der Trace-Log-Datei des ERA-Servers die neuesten Log-Einträge. Der Bericht enthält Empfehlungen zur Behebung des Problems. Die neueste Log-Datei des ERA-Servers befindet sich unter folgendem Pfad: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*

Erstellen Sie eine Dummy-Datei mit dem Namen **traceAll** ohne Erweiterung im gleichen Ordner wie die Datei trace.log, um vollständiges Logging zu aktivieren. Starten Sie den ESET Remote Administrator Server-Dienst neu, um das vollständige Logging in die Datei **trace.log** zu aktivieren.

2. Die folgende Tabelle enthält verschiedene Fehlerursachen bei der Agenten-Bereitstellung:

Fehlermeldung	Mögliche Ursache
Verbindung nicht möglich	Client ist im Netzwerk nicht erreichbar Client-Hostname konnte nicht aufgelöst werden Firewall blockiert die Kommunikation Die Ports 2222 und 2223 sind in der Firewall nicht geöffnet (auf Client- und Serverseite)
Zugriff verweigert	Kein Passwort für Administratorkonto festgelegt Unzureichende Zugriffsrechte Verwaltungsfreigabe ADMIN$ ist nicht verfügbar Verwaltungsfreigabe IPC$ ist nicht verfügbar Einfache Dateifreigabe ist aktiviert
Paket wurde nicht in Repository gefunden	Link zum Repository ist falsch Repository ist nicht verfügbar Repository enthält nicht das erforderliche Paket

3. Führen Sie je nach möglicher Ursache die entsprechenden Schritte zur Fehlerbehebung aus:

- Client nicht im Netzwerk erreichbar: Führen Sie vom ERA-Server einen Ping-Befehl zum Client aus. Wenn Sie eine Antwort erhalten, versuchen Sie, sich remote am Clientcomputer anzumelden (z. B. über Remote Desktop).
- Client-Hostname kann nicht aufgelöst werden: Für DNS-Probleme stehen unter anderem folgende Lösungsmöglichkeiten zur Verfügung:

  Verwenden Sie den Befehl `nslookup` für die IP-Adresse bzw. den Hostnamen des Servers und/oder der Clients, mit denen Probleme bei der Agenten-Bereitstellung auftreten. Die Ergebnisse müssen mit den Informationen vom entsprechenden Computer übereinstimmen. Beispielsweise sollte über den Befehl `nslookup` für einen Hostnamen die IP-Adresse angezeigt werden, die vom Befehl `ipconfig` auf dem betroffenen Host angezeigt wird. Der Befehl `nslookup` muss auf den Clients und auf dem Server ausgeführt werden.

  Überprüfen Sie die DNS-Einträge manuell auf Duplikate.
- Firewall blockiert die Kommunikation: Überprüfen Sie die Einstellungen der Firewall auf dem Server und auf dem Client und, sofern zutreffend, aller anderen Firewalls zwischen den beiden Computern.
- Die Ports 2222 und 2223 sind in der Firewall nicht geöffnet: Vergewissern Sie sich, dass diese Ports in allen Firewalls zwischen den beiden Computern (Client und Server) geöffnet sind.
- Kein Passwort für Administratorkonto festgelegt: Legen Sie ein zulässiges Passwort für das Administratorkonto fest (verwenden Sie keine leeren Passwörter).
- Unzureichende Zugriffsrechte: Versuchen Sie, den Task für die Agenten-Bereitstellung mit den Anmeldedaten des Domänenadministrators auszuführen. Wenn sich der Clientcomputer in einer Arbeitsgruppe befindet, verwenden Sie auf diesem Computer das lokale Administratorkonto.
- Die Verwaltungsfreigabe ADMIN$ ist nicht verfügbar: Auf dem Clientcomputer muss die freigegebene Ressource ADMIN$ aktiviert sein. Vergewissern Sie sich, dass sie in den anderen Freigaben enthalten ist (**Start** > **Systemsteuerung** > **Verwaltung** > **Computerverwaltung** > **Freigegebene Ordner** > **Freigaben**).
- Die Verwaltungsfreigabe IPC$ ist nicht verfügbar: Vergewissern Sie sich, dass der Client auf IPC zugreifen kann, indem Sie in der Eingabeaufforderung auf dem Client Folgendes eingeben:

```
net use \\servername\IPC$
```

servername muss durch den Namen des ERA-Servers ersetzt werden.

- Einfache Dateifreigabe ist aktiviert: Wenn Sie die Fehlermeldung „Zugriff verweigert“ erhalten und in einer gemischten Umgebung aus Domänen und Arbeitsgruppen arbeiten, deaktivieren Sie auf allen Computern, auf denen Probleme bei der Agenten-Bereitstellung auftreten, die Funktion **Einfache Dateifreigabe verwenden** bzw. **Freigabe-Assistent verwenden**. Gehen Sie unter Windows 7 beispielsweise folgendermaßen vor:
    - Klicken Sie auf **Start**, geben Sie `Ordner` in das Suchfeld ein und klicken Sie dann auf **Ordneroptionen**. Klicken Sie auf die Registerkarte **Ansicht** und blättern Sie unter „Erweiterte Einstellungen“ nach unten. Deaktivieren Sie das Kontrollkästchen **Freigabe-Assistent verwenden**.

- Falscher Link zum Repository: Navigieren Sie in der Web-Konsole zu **Admin** > **Servereinstellungen,** klicken Sie auf **Erweiterte Einstellungen** > **Repository** und vergewissern Sie sich, dass die Repository-URL richtig ist.
- Paket nicht im Repository gefunden: Diese Fehlermeldung wird üblicherweise angezeigt, wenn keine Verbindung zum ERA-Repository hergestellt werden kann. Überprüfen Sie die Internetverbindung.

HINWEIS: Auf neueren Windows-Betriebssystemen (Windows 7, Windows 8 usw.) muss das Administrator-Benutzerkonto aktiviert sein, um den Task für die Agenten-Bereitstellung auszuführen.

So aktivieren Sie das Administrator-Benutzerkonto:
1. Öffnen Sie als Administrator ein Eingabeaufforderungsfenster.
2. Geben Sie den folgenden Befehl ein: `net user administrator /active:yes`

Linux und Mac OS

Wenn bei der Agenten-Bereitstellung auf einem Linux- oder Mac OS-Betriebssystem Probleme auftreten, liegt dies üblicherweise an einem Problem mit SSH. Überprüfen Sie den Clientcomputer und vergewissern Sie sich, dass der SSH-Daemon ausgeführt wird. Führen Sie dann erneut die Agenten-Bereitstellung aus.

4.4.3 Agenten-Bereitstellung mithilfe von GPO und SCCM

Nach der erfolgreichen Installation von ESET Remote Administrator müssen der **ERA-Agent** und ESET-Sicherheitsprodukte auf den Computern im Netzwerk bereitgestellt werden.

Alternativ zur lokalen oder Remote-Bereitstellung per Servertask können Sie auch Verwaltungswerkzeuge wie GPO, SCCM, Symantec Altiris oder Puppet verwenden. Klicken Sie auf den entsprechenden Link für schrittweise Anweisungen für zwei beliebte Bereitstellungsmethoden für den ERA-Agenten:

1. Bereitstellung des ERA-Agenten mit GPO

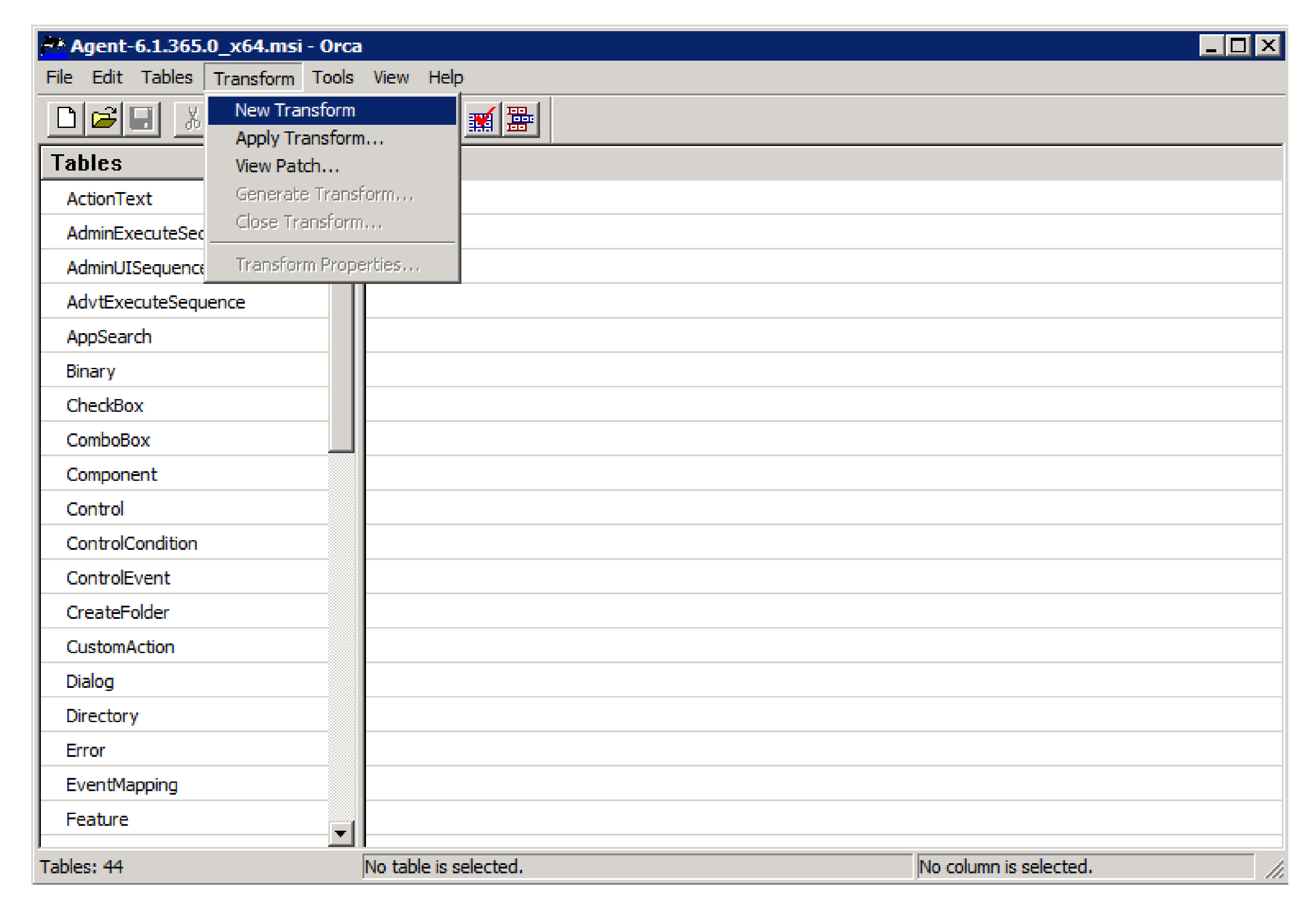
2. Bereitstellung des ERA-Agenten mit SCCM

4.4.3.1 Erstellen der MST-Datei

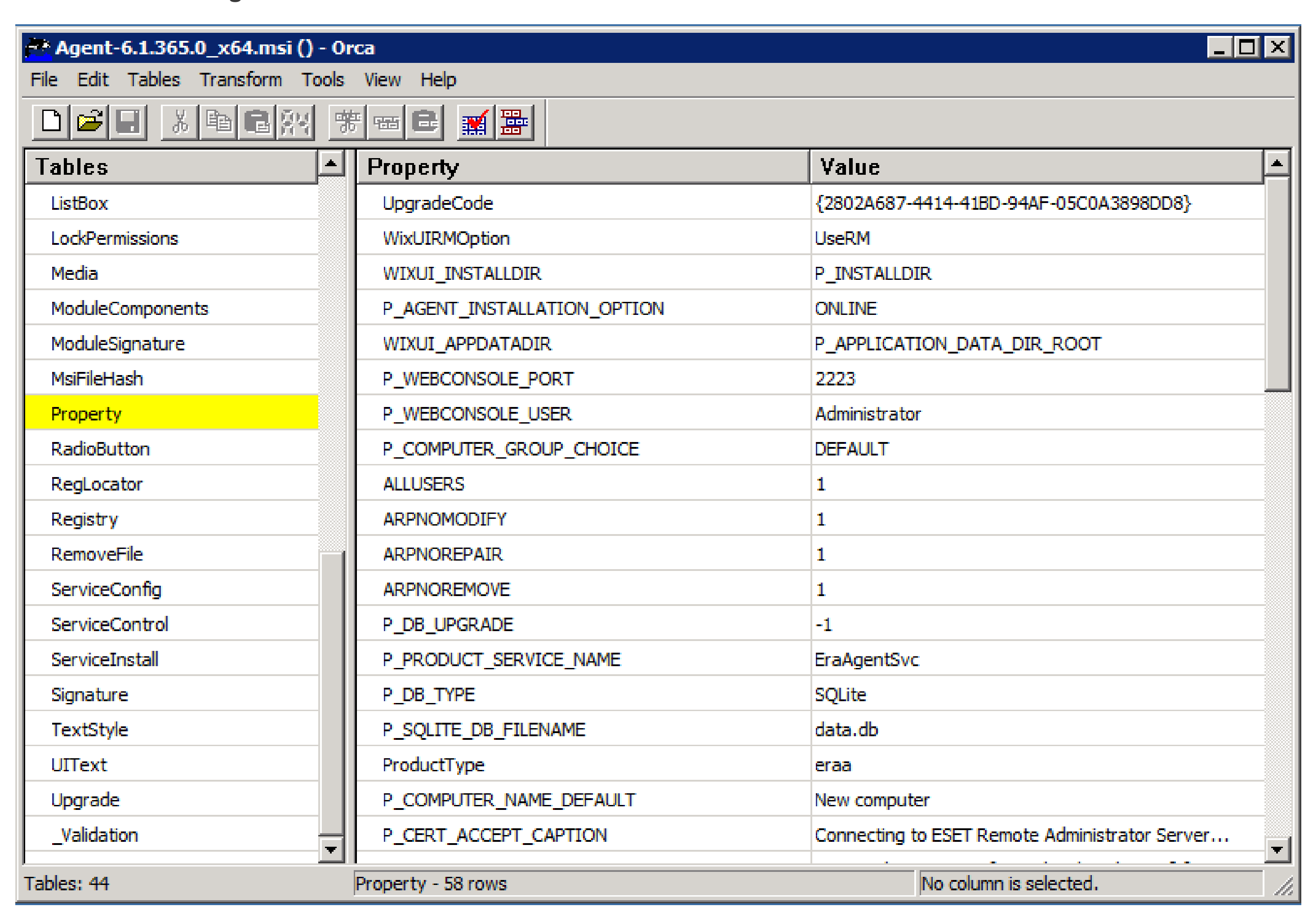
Vor der Bereitstellung der Installationsdatei für den ERA-Agenten müssen Sie eine `.mst`- Transformationsdatei mit Einstellungen für den ERA-Agenten erstellen. Führen Sie die folgenden Schritte aus oder lesen Sie unseren Knowledgebase-Artikel, um die Transformationsdatei zu erstellen.

1. Installieren Sie Orca (im Windows SDK enthalten). Weitere Informationen zu Orca finden Sie unter http://support.microsoft.com/kb/255905/
2. Laden Sie das Installationsprogramm für den **ERA-Agenten** herunter. Sie können zum Beispiel `Agent-6.1.365.0_x64.msi` verwenden, eine Komponente der ERA-Version 6.1.28.0 für 64-Bit-Systeme. In unserem Knowledgebase-Artikel finden Sie eine Liste der ERA-Komponentenversionen.
3. Öffnen Sie Orca, indem Sie auf Start > **Programme** > **Orca** klicken.

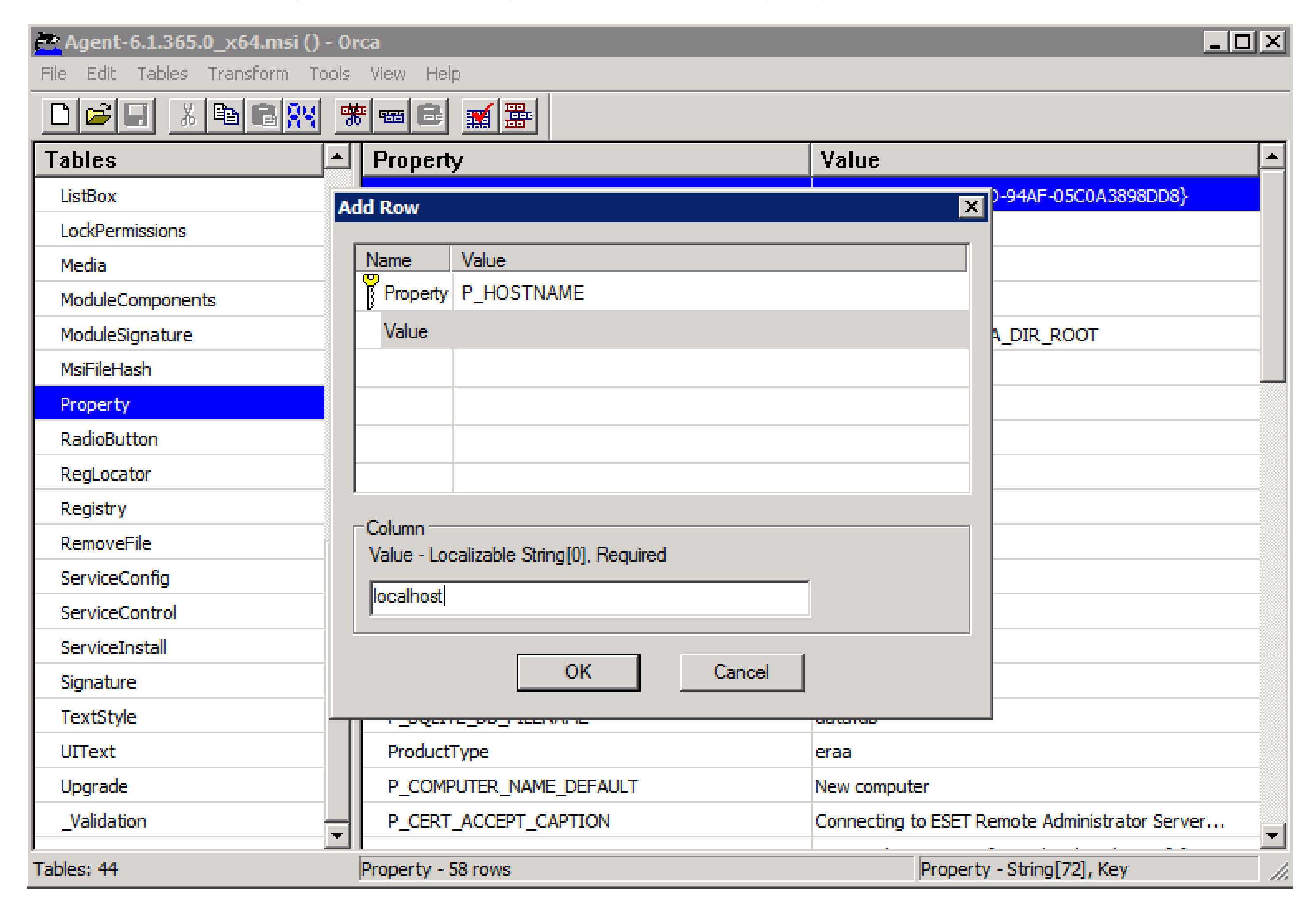
4. Klicken Sie im Menü auf **Datei** > **Öffnen** und navigieren Sie zur Datei `Agent-6.1.365.0_x64.msi`.
5. Klicken Sie in der oberen Menüleiste auf **Transformation** und wählen Sie **Neue Transformation** aus.



6. Klicken Sie auf **Eigenschaft**.



7. Klicken Sie mit der rechten Maustaste in die Liste der Eigenschaftswerte und wählen Sie den Eintrag **Zeile hinzufügen** im Kontextmenü aus.
8. Fügen Sie die Eigenschaft **P_HOSTNAME** hinzu und geben Sie den Hostnamen oder die IP-Adresse Ihres ERA-Servers in das Feld **Wert** ein.
9. Wiederholen Sie die Schritte 7 und 8 und erstellen Sie die Eigenschaft P_PORT. Verwenden Sie als Wert den Port, den Sie standardmäßig für die Verbindung mit Ihrem ERA-Server (2222) verwenden.

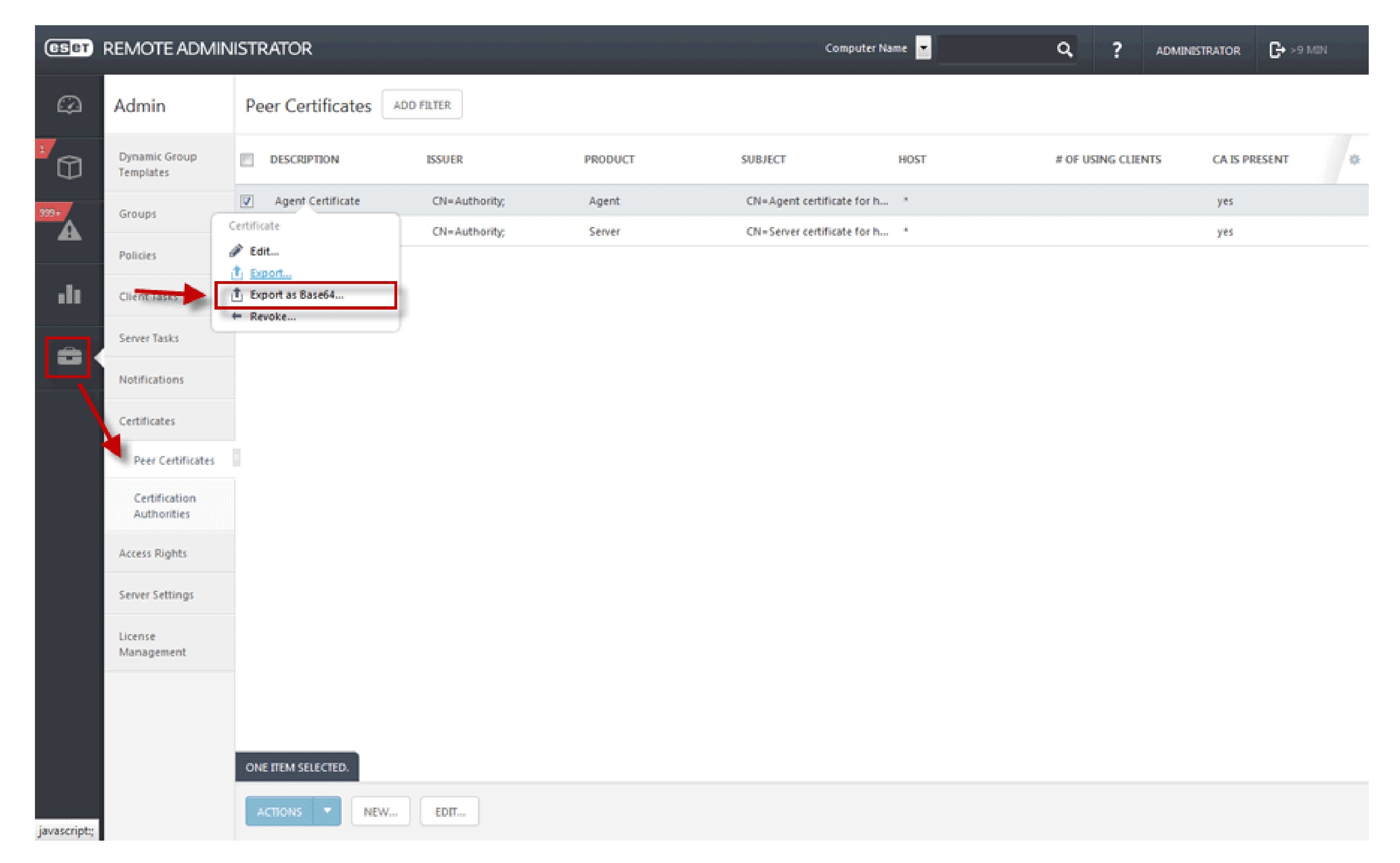


10. Fügen Sie für den ERA-Agenten das von Ihrer Zertifizierungsstelle signierte Peerzertifikat (.pfx) ein, das in der ERA Server-Datenbank gespeichert ist. Fügen Sie den öffentlichen Schlüssel der Zertifizierungsstelle ein (`.der`-Datei), mit dem Ihr ERA Server-Peerzertifikat signiert wurde.

- **Zertifikate können auf zwei Arten eingefügt werden:**

1. Sie können den Inhalt des Zertifikats und den öffentlichen Schlüssel im **Base64-Format** codiert einfügen (keine Zertifikatdatei benötigt).

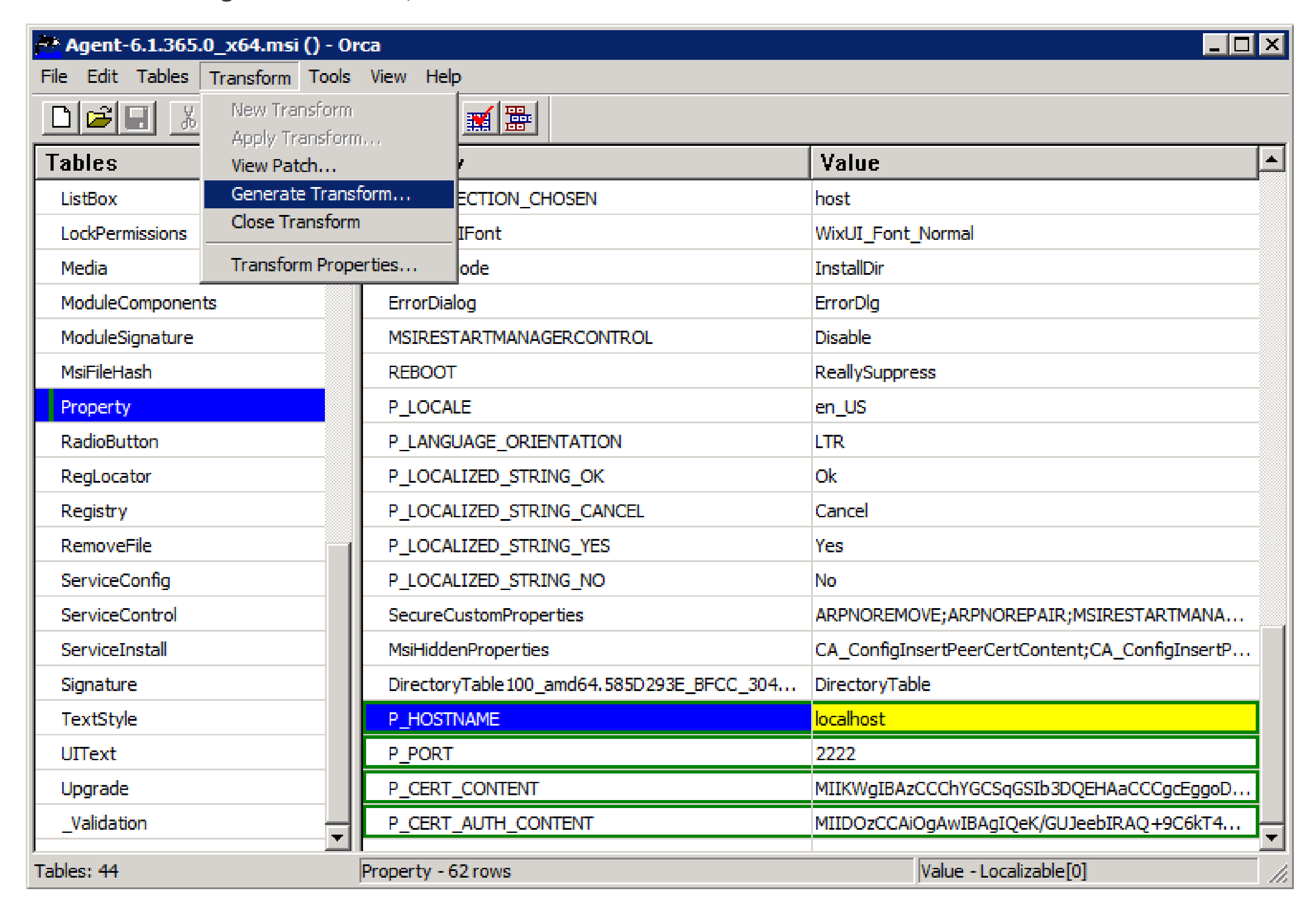
- Navigieren Sie in der ERA Web-Konsole zu **Admin** > **Zertifikate** > **Peerzertifikat**, klicken Sie auf Agentenzertifikat und wählen Sie **Als Base64 exportieren..** aus.
- Navigieren Sie zu **Admin** > **Zertifikate** > **Zertifizierungsstellen**, klicken Sie auf ERA-Zertifizierungsstelle und wählen Sie **Öffentlichen Schlüssel als Base64 exportieren**



- Fügen Sie den Inhalt des exportierten Zertifikats und den öffentlichen Schlüssel mit den folgenden Eigenschaftennamen in die Eigenschaftentabelle in Orca ein:

Eigenschaftenname	Wert
P_CERT_CONTENT	<Peerzertifikat im Base64-Format>
P_CERT_PASSWORD	<Passwort für das Peerzertifikat (nicht hinzufügen, falls das Passwort leer ist)>
P_CERT_AUTH_CONTENT	<exportierter öffentlicher Schlüssel der Zertifizierungsstelle im Base64-Format>

- Neue Eigenschaften werden in grüner Farbe hinterlegt. Klicken auf **Transformieren** und wählen Sie **Transformation generieren...** aus, um eine `.mst` -Datei zu erstellen.

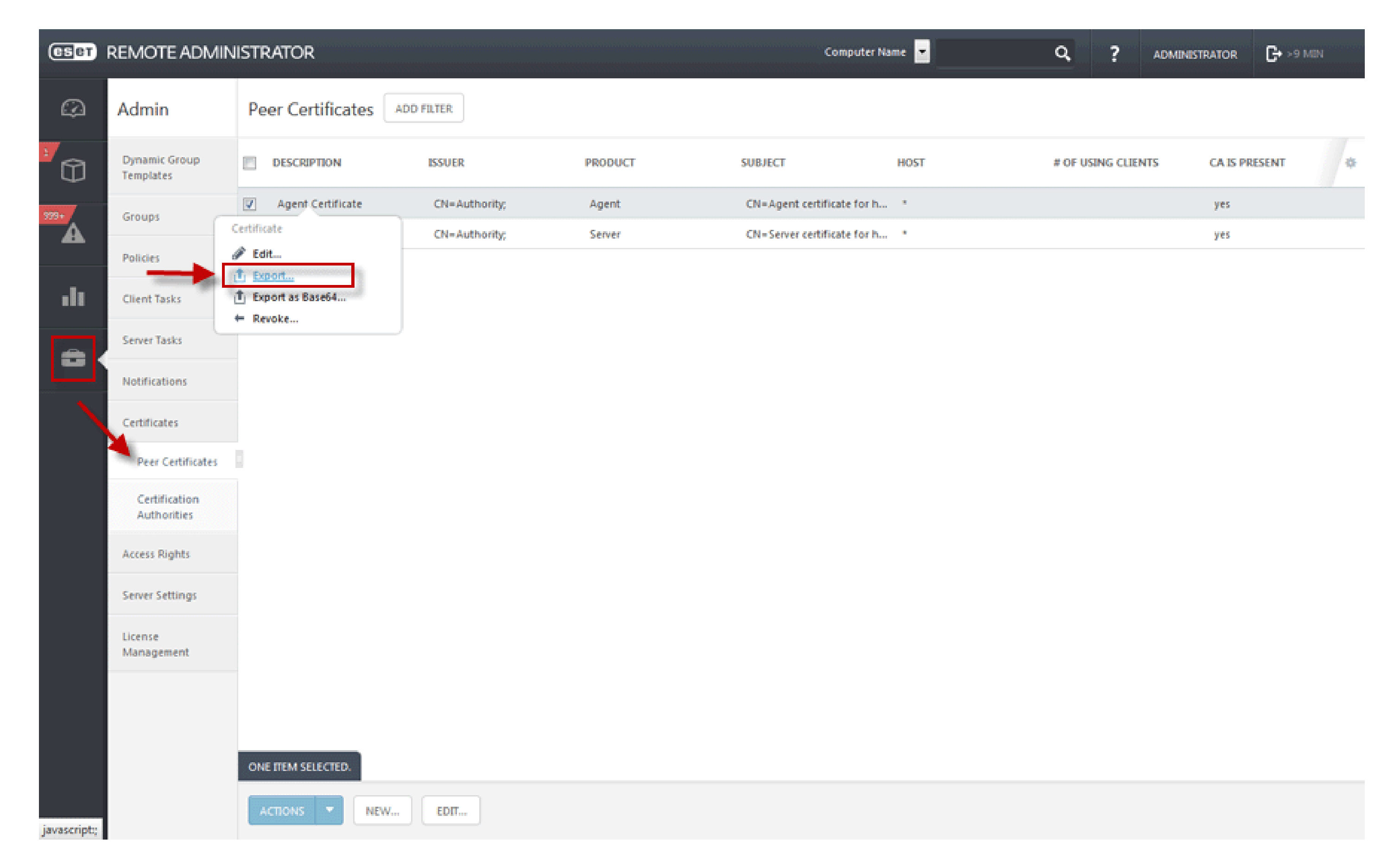


2. Sie können die Zertifikatdateien herunterladen und vom Zielcomputer aus erreichbar machen. Exportieren Sie das **Agenten-Peerzertifikat** und die **öffentliche Schlüssel-**Datei in der **Zertifizierungsstelle** von ERA Server und legen Sie beide Dateien in einem Ordner ab, der für den Zielcomputer erreichbar ist, auf dem der ERA-Agent installiert wird.

HINWEIS: Diese Option wird in Sonderfällen **empfohlen**.

- Navigieren Sie zu **Admin** > **Zertifikate** > **Peerzertifikat**, klicken Sie auf **Agentenzertifikat** und wählen Sie **Exportieren... aus.**

- Navigieren Sie zu **Admin** > **Zertifikate** > **Zertifizierungsstellen**, klicken Sie auf **ERA-Zertifizierungsstelle** und wählen Sie **Öffentlichen Schlüssel exportieren aus**



- Verwenden Sie die exportierten Dateien und fügen Sie deren Pfad mit den folgenden Eigenschaftennamen in die Eigenschaftentabelle in Orca ein:

Eigenschaftenname	Wert
P_CERT_PATH	<Pfad des exportierten `.pfx`- Zertifikats
P_CERT_PASSWORD	<Passwort für das `.pfx`- Zertifikat (nicht hinzufügen, falls das Passwort leer ist)>
P_CERT_AUTH_PATH	<Pfad zum exportierten öffentlichen Schlüssel der Zertifizierungsstelle>

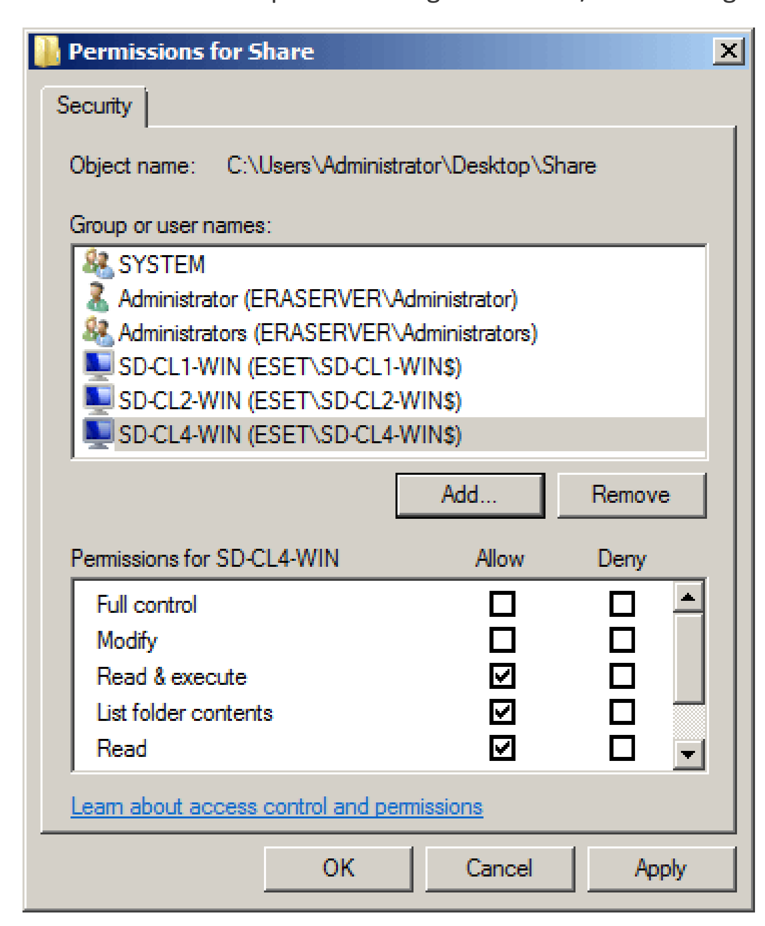
- Die neuen Eigenschaften werden in grüner Farbe hinterlegt. Klicken auf **Transformieren** und wählen Sie **Transformation generieren...** aus, um eine `.mst` -Datei auszuwählen.

4.4.3.2 Bereitstellungsschritte – GPO

Führen Sie die folgenden Schritte aus oder lesen Sie unseren Knowledgebase-Artikel für die Bereitstellung des ERA-Agenten mithilfe von GPO:

1. Laden Sie das Installationsprogramm für den ERA-Agenten herunter `(.msi)` Datei von der ESET-Downloadseite.
2. Erstellen Sie eine .mst-Transformationsdatei für das ERA-Agenten-Installationsprogramm.
3. Speichern Sie das Installationsprogramm für den ERA-Agenten `(.msi)` und die Transformationsdatei `(.mst)` in einem freigegebenen Ordner, der von Ihren Zielclients aus erreichbar ist.

HINWEIS: Clientcomputer benötigen Schreib-/Ausführungszugriff für diesen freigegebenen Ordner.



4. Verwenden Sie ein vorhandenes Gruppenpolicy-Objekt oder erstellen Sie ein neues Objekt (klicken Sie mit der rechten Maustaste auf GPO und anschließend auf **Neu**). Klicken Sie in der Struktur der GPMC (Gruppenpolicy-Verwaltungskonsole) mit der rechten Maustaste auf die GPO, die Sie verwenden möchten, und klicken Sie auf **Bearbeiten**...

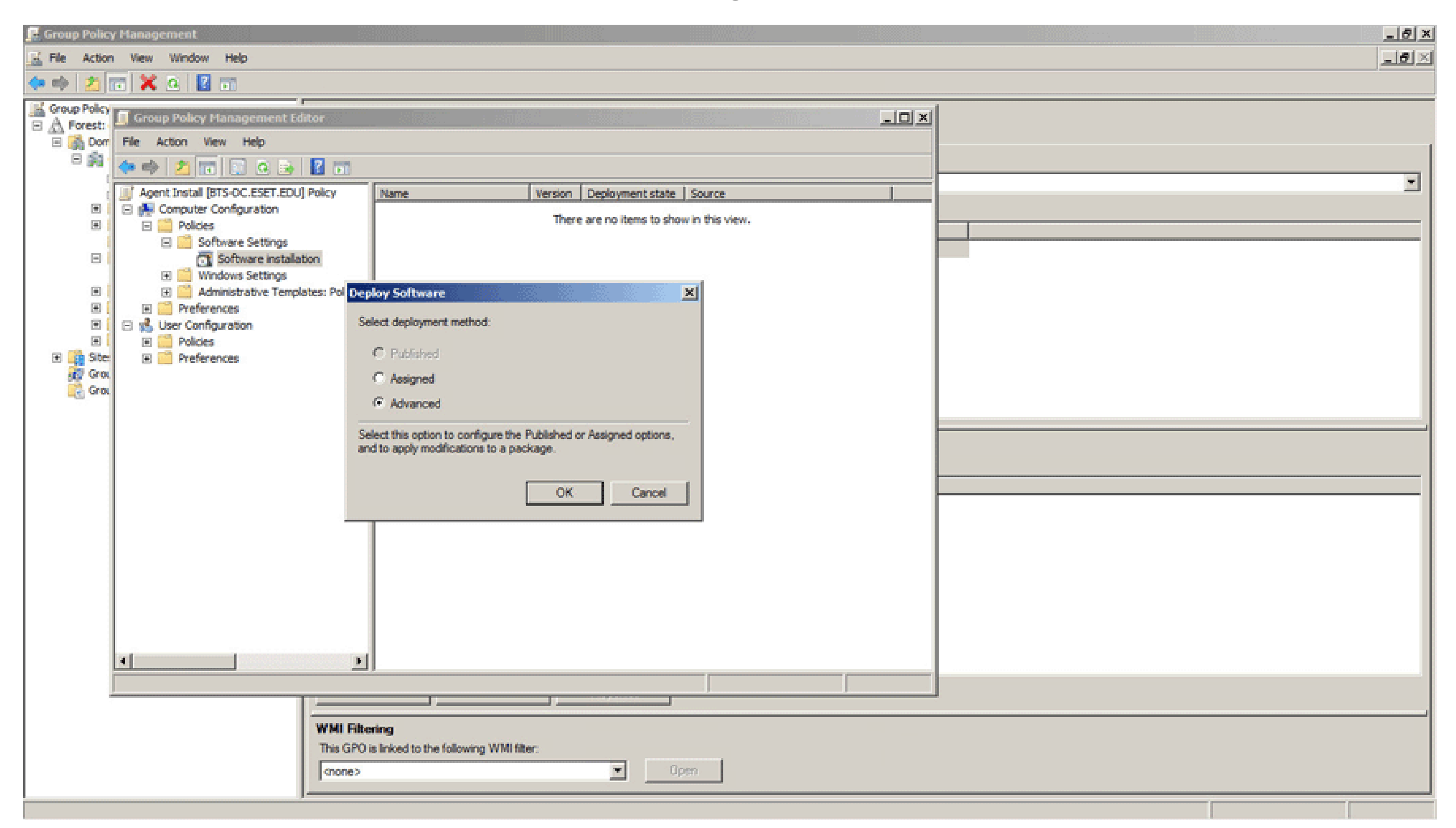
5. Navigieren Sie in der Computer-Konfiguration zu **Policies** > **Softwareeinstellungen** > **Softwareeinstellungen**.

6. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation**, wählen Sie **Neu** aus und klicken Sie auf **Paket**..., um eine neue Paketkonfiguration zu erstellen.

7. Navigieren Sie zum Speicherort der `(.msi)` -Datei des ERA-Agenten. Geben Sie im Dialogfeld "Öffnen" den Universal Naming Convention (UNC)-Pfad des freigegebenen Installationspakets ein, das Sie verwenden möchten. Zum Beispiel: `\\fileserver\share\filename.msi`

HINWEIS: Verwenden Sie unbedingt den UNC-Pfad des freigegebenen Installationspakets.

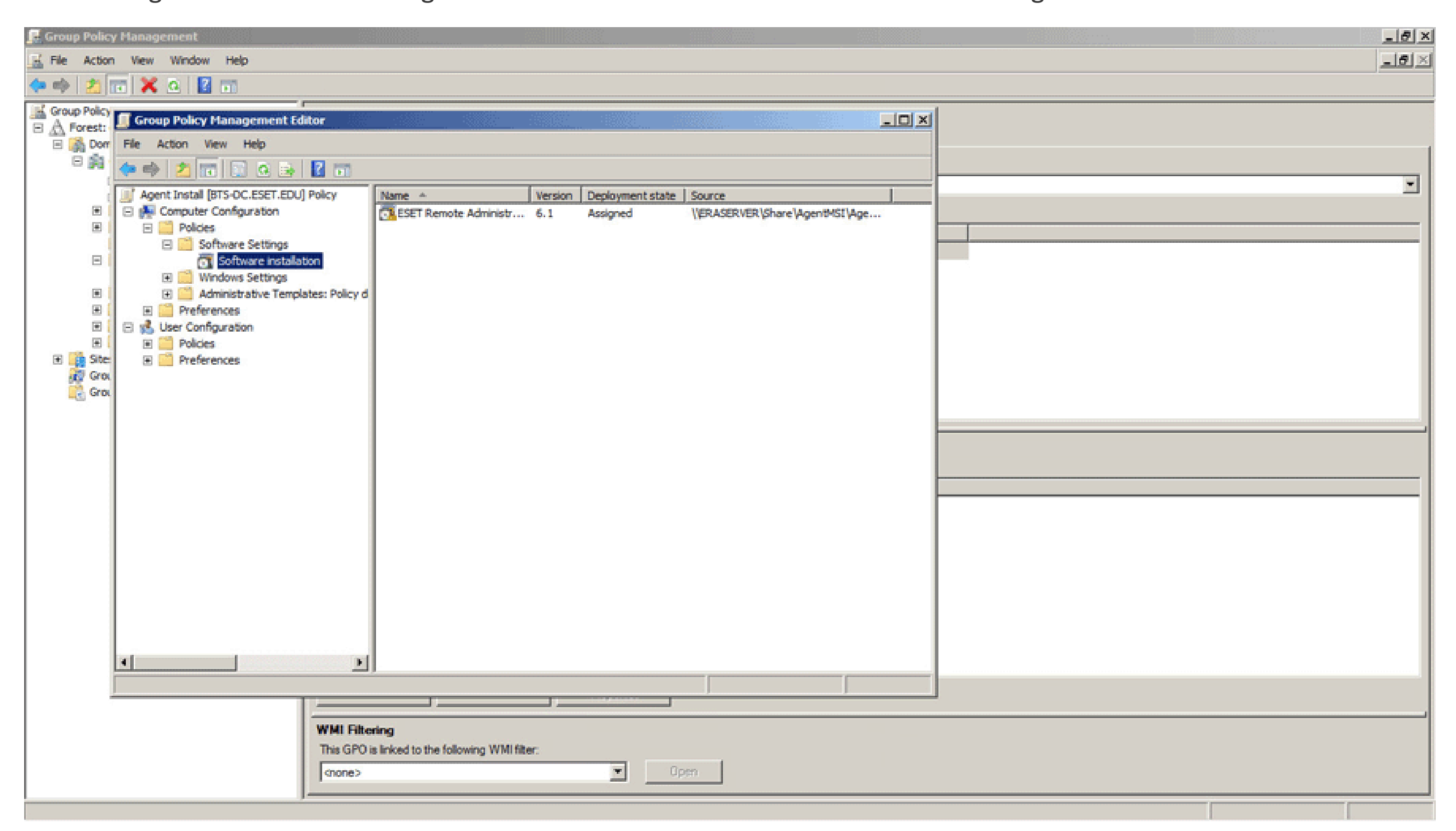
8. Klicken Sie auf **Öffnen** und wählen Sie die Bereitstellungsmethode **Erweitert** aus.



9. Mit dieser Methode können Sie Bereitstellungsoptionen konfigurieren. Wechseln Sie zur Registerkarte **Modifikationen** und navigieren Sie zur `.mst`- Transformationsdatei für das Installationsprogramm des ERA-Agenten.

HINWEIS: Der Pfad muss auf denselben freigegebenen Ordner zeigen wie in Schritt 7.

10. Bestätigen Sie die Paketkonfiguration und fahren Sie mit der GPO-Bereitstellung fort.

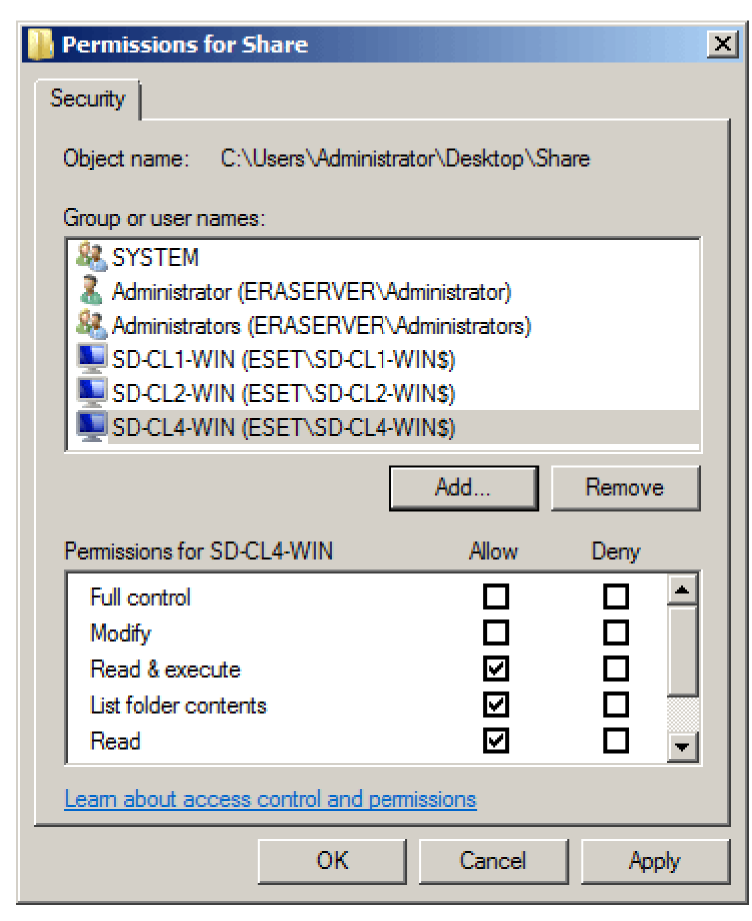


4.4.3.3 Bereitstellungsschritte – SCCM

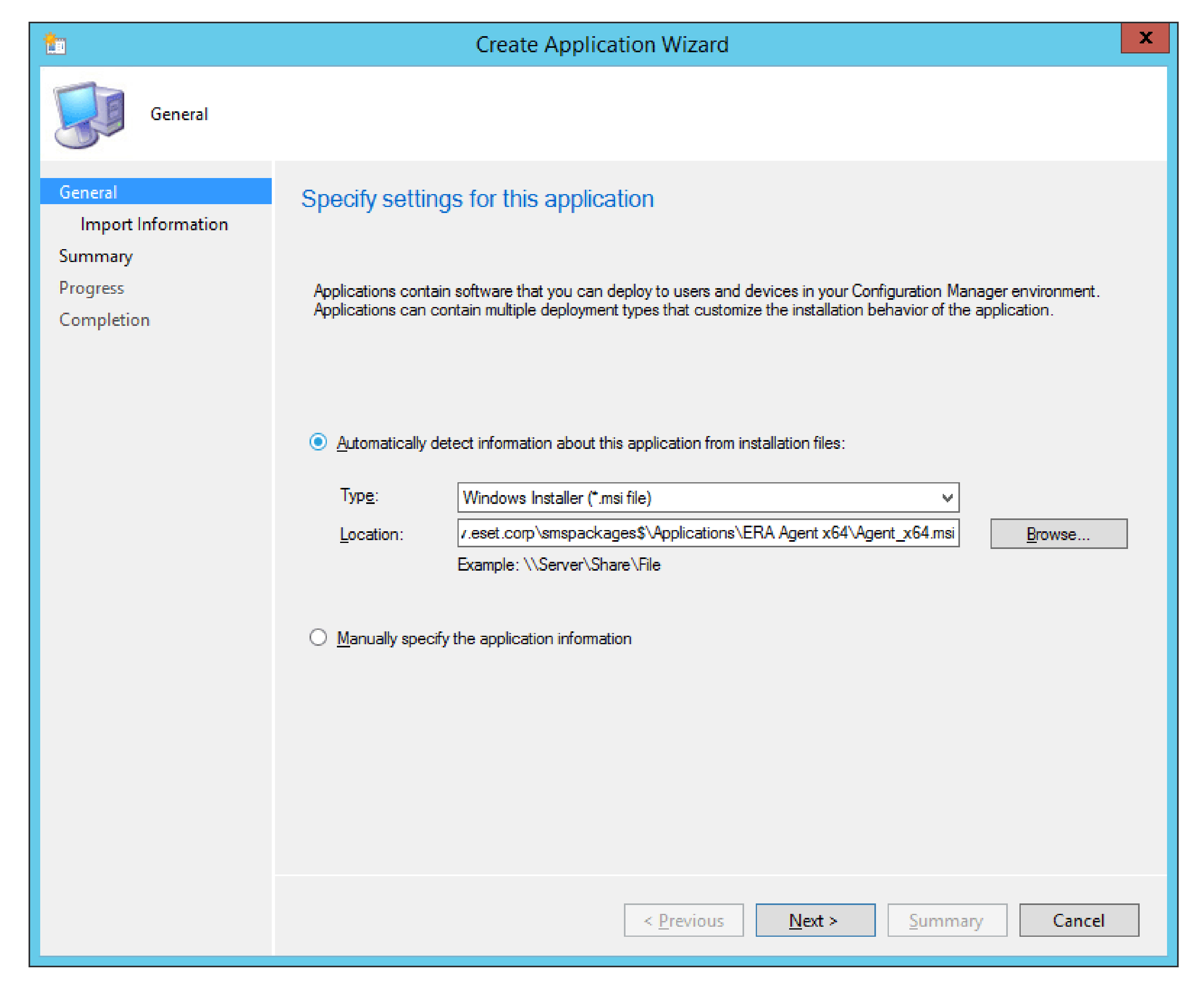
Führen Sie die folgenden Schritte aus oder lesen Sie unseren Knowledgebase-Artikel für die Bereitstellung des ERA-Agenten mithilfe von SCCM:

1. Laden Sie das Installationsprogramm für den ERA-Agenten herunter `.msi`- Datei von der ESET-Downloadseite.
2. Erstellen Sie eine .mst-Transformationsdatei für das ERA-Agenten-Installationsprogramm.
3. Speichern Sie das Installationsprogramm für den ERA-Agenten `(.msi)` und die Transformationsdatei `(.mst)` in einem freigegebenen Ordner.

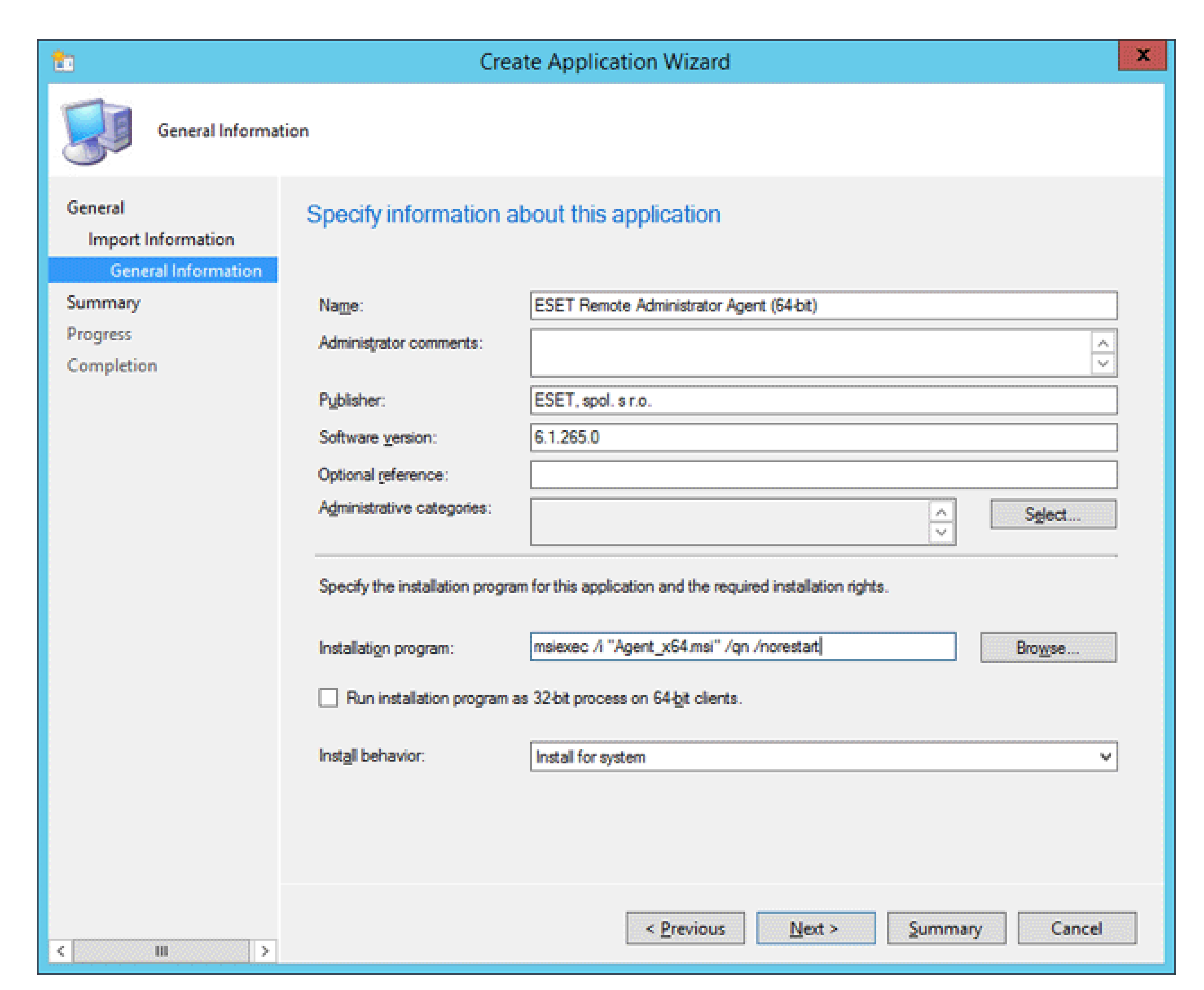
HINWEIS: Clientcomputer benötigen Schreib-/Ausführungszugriff für diesen freigegebenen Ordner.



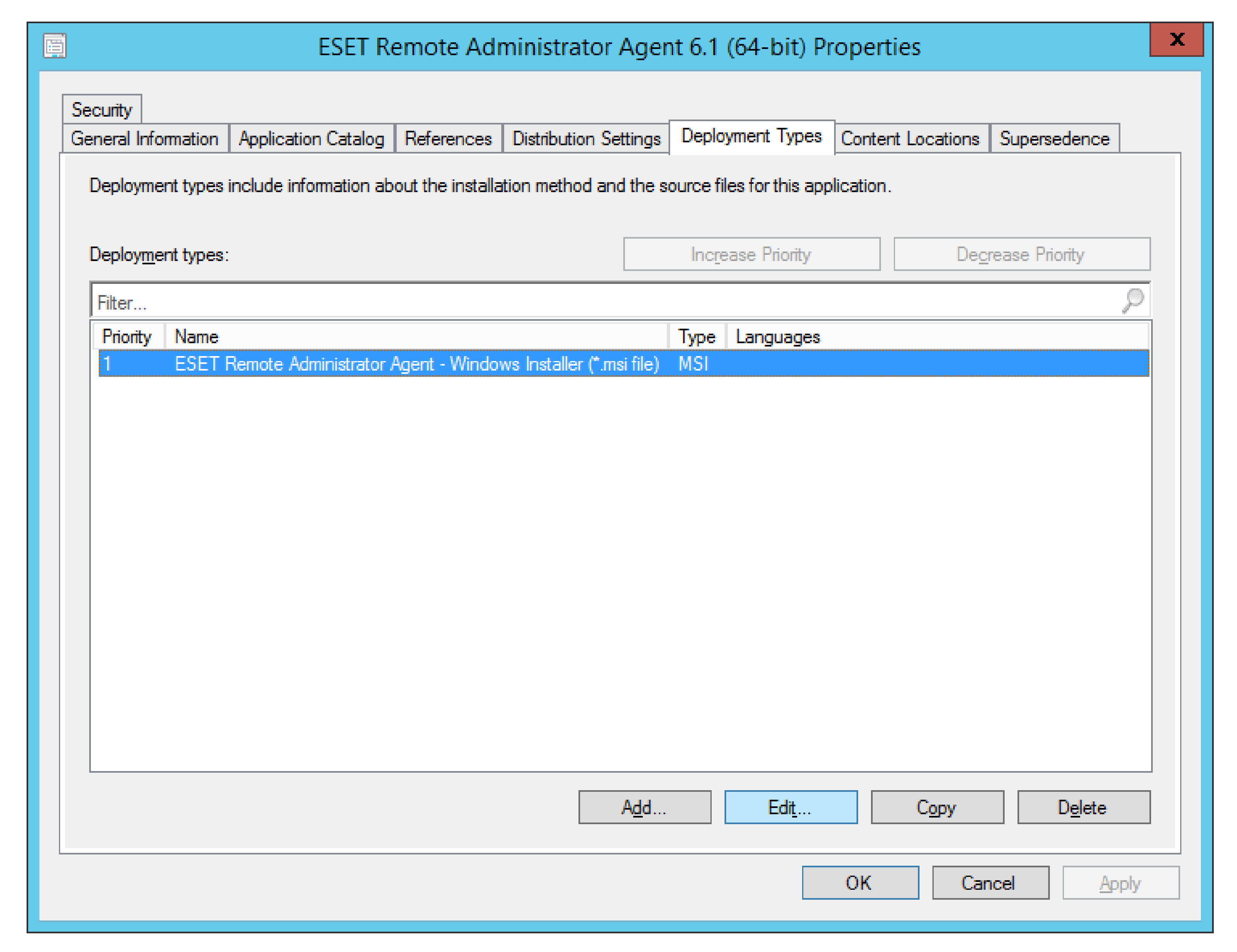
4. Öffnen Sie die SCCM-Konsole und klicken Sie auf **Softwarebibliothek**. Klicken Sie unter **Anwendungsverwaltung** mit der rechten Maustaste auf **Anwendungen** und anschließend auf **Anwendung erstellen**. Wählen Sie **Windows Installer (*.msi-Datei)** aus und navigieren Sie zum Quellordner, in dem Sie das Installationsprogramm für den ERA-Agenten `(.msi)` gespeichert haben.



5. Füllen Sie alle benötigten Informationen über die Anwendung aus und klicken Sie auf **Weiter**.

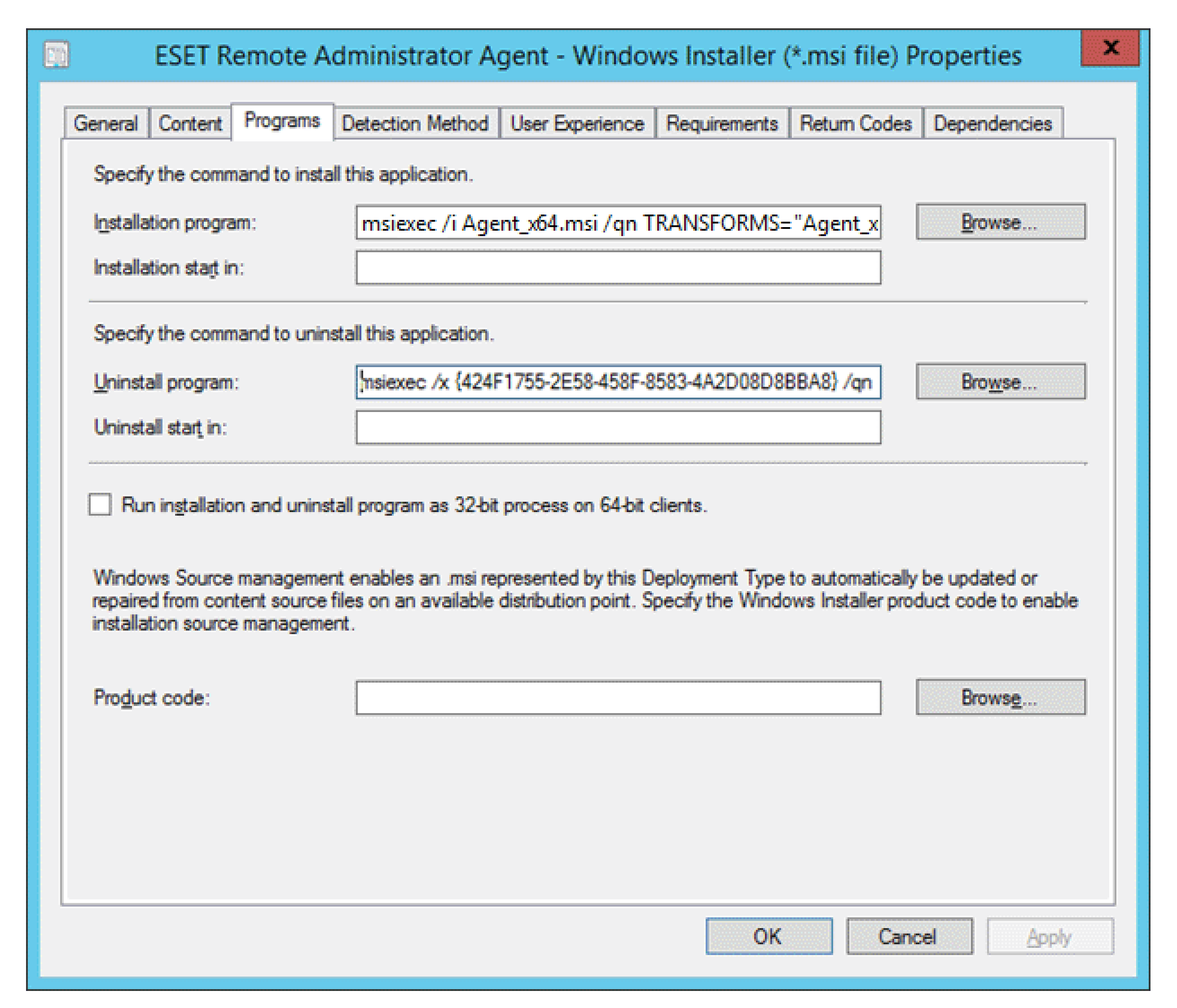


6. Klicken Sie mit der rechten Maustaste auf die ESET Remote Administrator Agenten-Anwendung, klicken Sie auf die Registerkarte **Bereitstellungstypen**, wählen Sie die einzige angezeigte Bereitstellung aus und klicken Sie auf **Bearbeiten**.

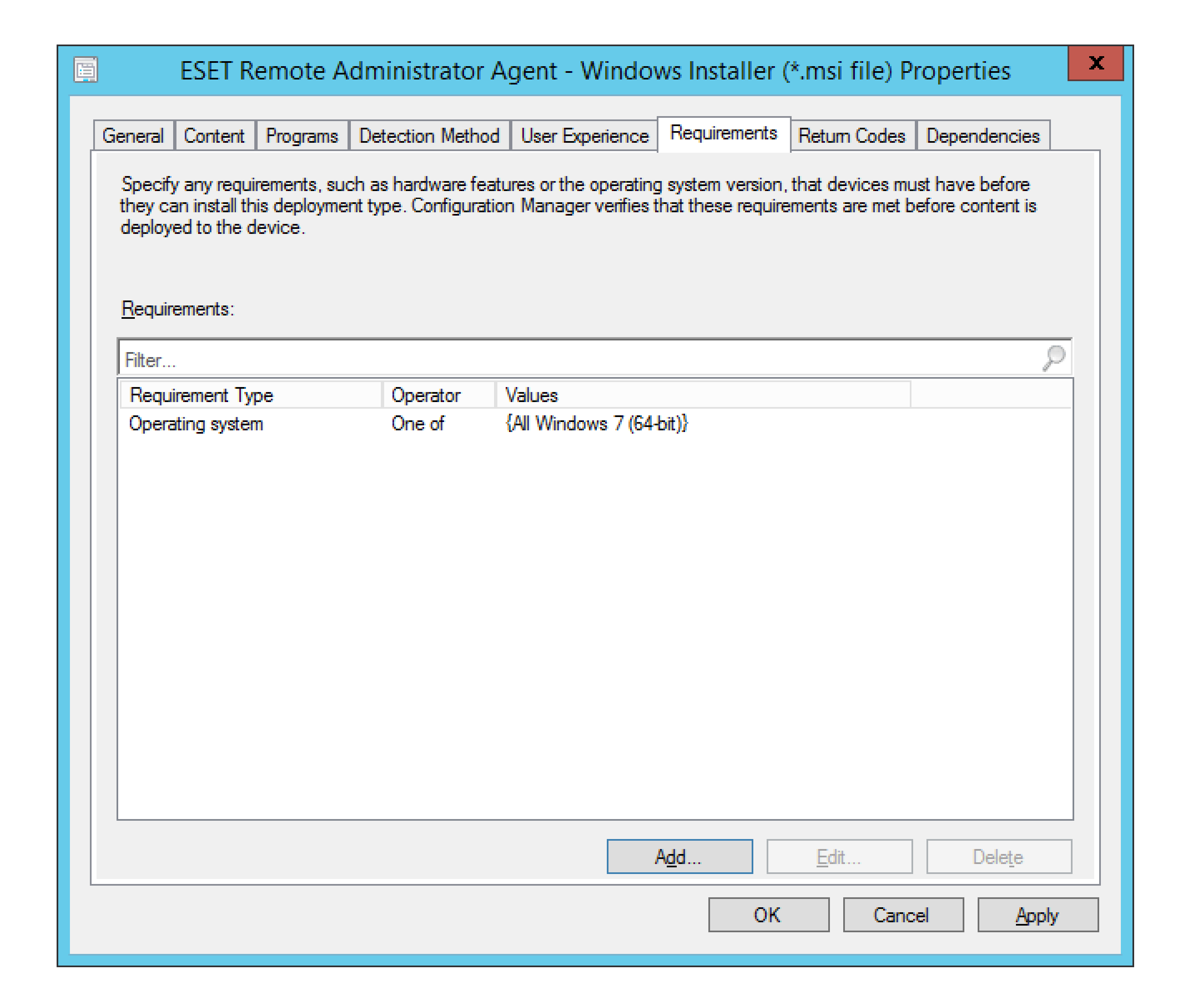


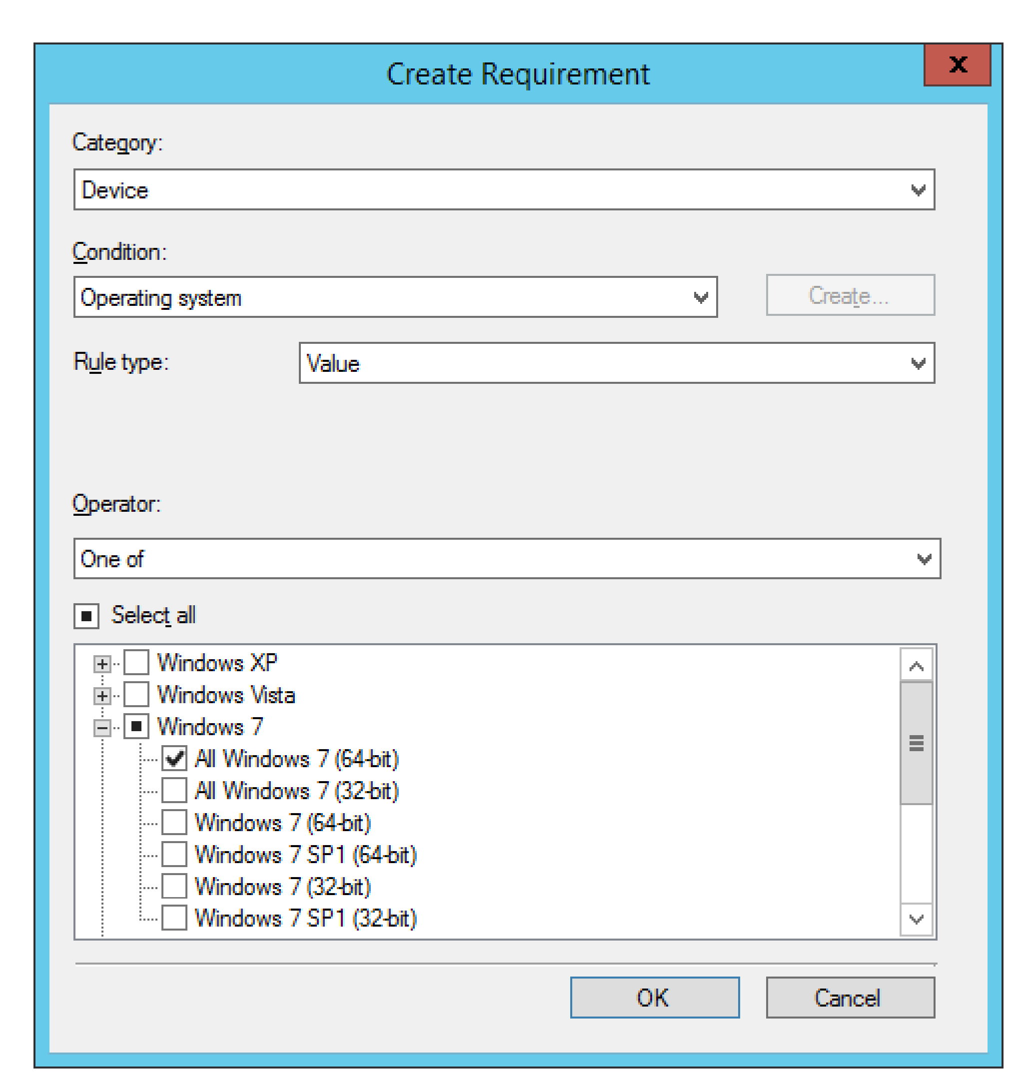
7. Klicken Sie auf die Registerkarte "Programme" und fügen Sie den Wert msiexec/iAgent_x64.msi/qn TRANSFORMS="Agent_x64.mst in das Feld "Installationsprogramm" ein (wenn Sie 32-Bit-Pakete verwenden, enthält diese Zeichenfolge "x32" an der Stelle von "x64" im gezeigten Beispiel).

8. Fügen Sie den Wert "msiexec/x {424F1755-2E58-458F-8583-4A2D08D8BBA8} /qn/norestart" in das Feld "Deinstallationsprogramm" ein.

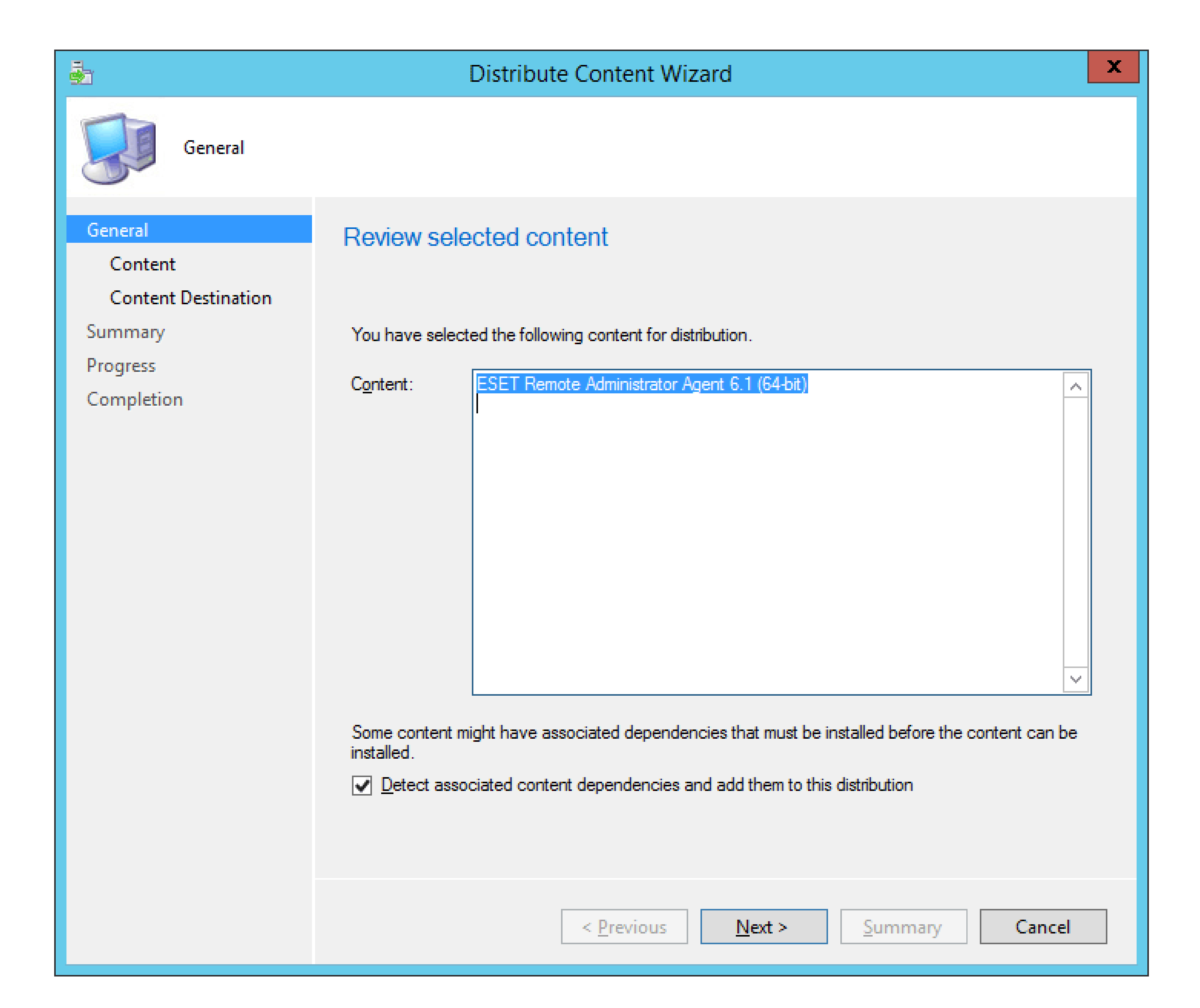


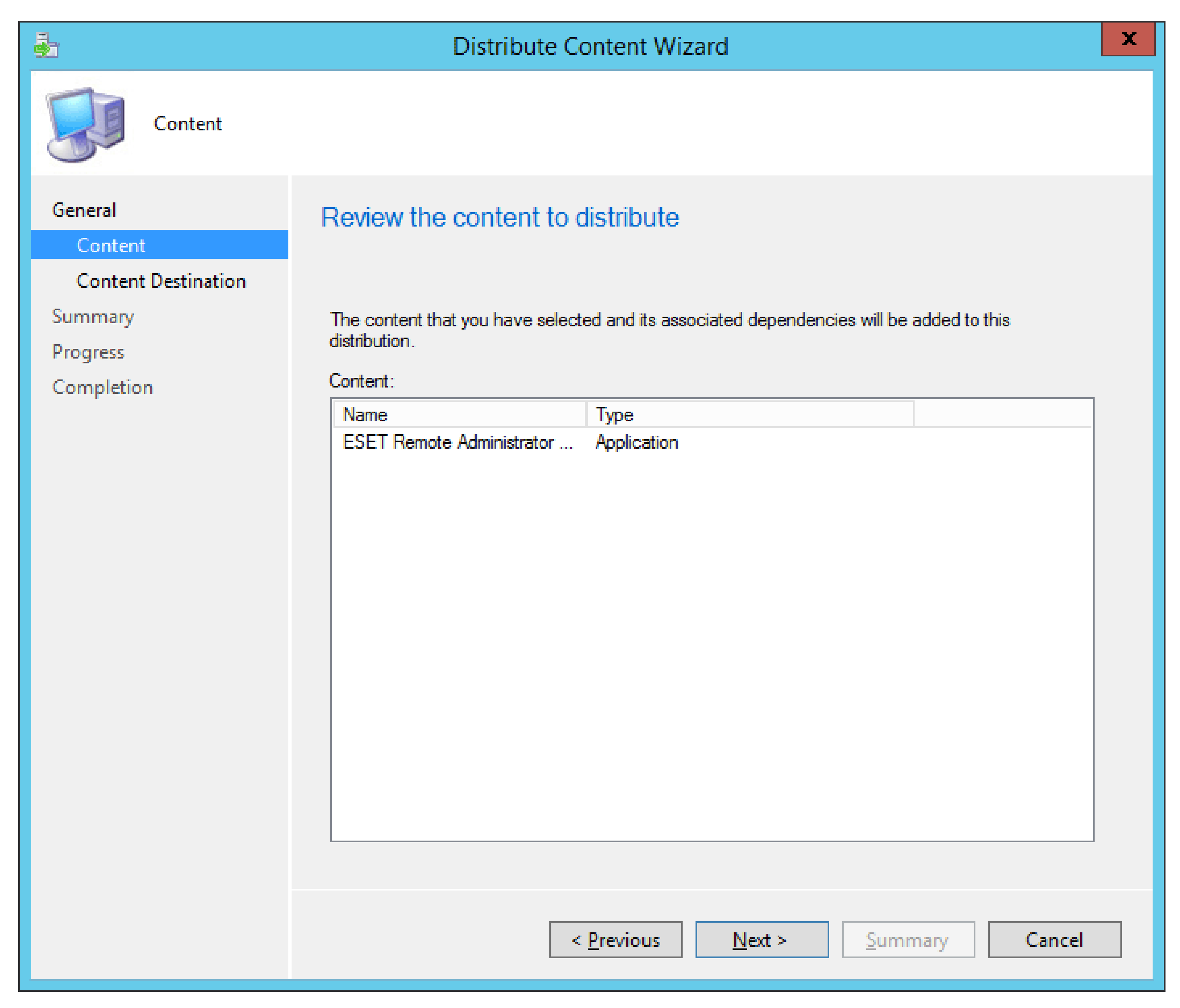
9. Klicken Sie auf die Registerkarte **Anforderungen** und anschließend auf "Hinzufügen". Wählen Sie "Betriebssystem" im Dropdownmenü "Bedingung" aus, wählen Sie ein Betriebssystem im Dropdownmenü "Operator" aus und markieren Sie die entsprechenden Kontrollkästchen, um die Zielbetriebssysteme für die Installation auszuwählen. Klicken Sie auf OK, wenn Sie fertig sind, und anschließend auf OK, um alle verbleibenden Fenster zu schließen und Ihre Änderungen zu speichern.


ESET Remote Administrator Agent - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 7 (64-bit)}
Add...
Edit...
Delete
OK
Cancel
Apply

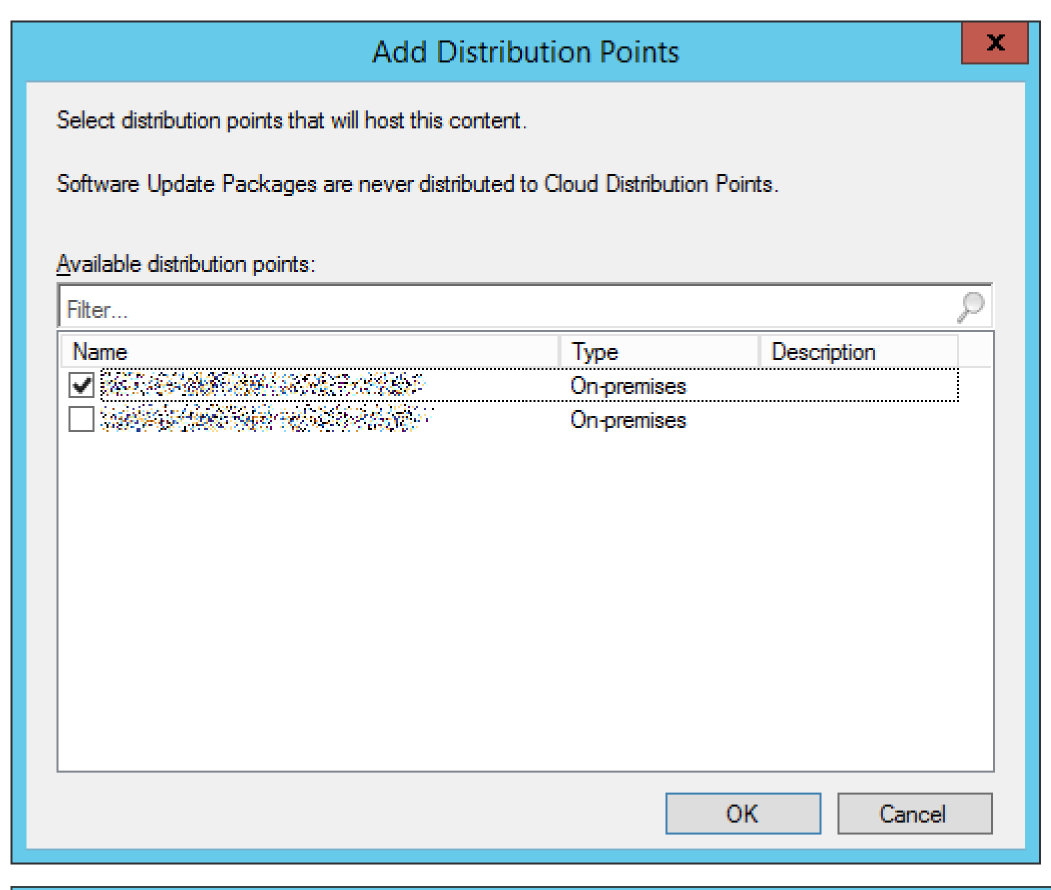


10. Klicken Sie in der System Center-Softwarebibliothek mit der rechten Maustaste auf Ihre neue Anwendung und wählen Sie den Eintrag "Inhalt verteilen" im Kontextmenü aus. Folgen Sie den Aufforderungen im Bereitstellungs-Assistenten, um die Bereitstellung der Anwendung abzuschließen.


Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent 6.1 (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel



11. Klicken Sie mit der rechten Maustaste auf die Anwendung und wählen Sie **Bereitstellen** aus. Führen Sie den Assistenten aus und wählen Sie die Auflistung und das Ziel für die Bereitstellung des Agenten aus.



Distribute Content Wizard

Content Destination

General

Content

Content Destination

Summary

Progress

Completion

Specify the content destination

Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

Content destination:

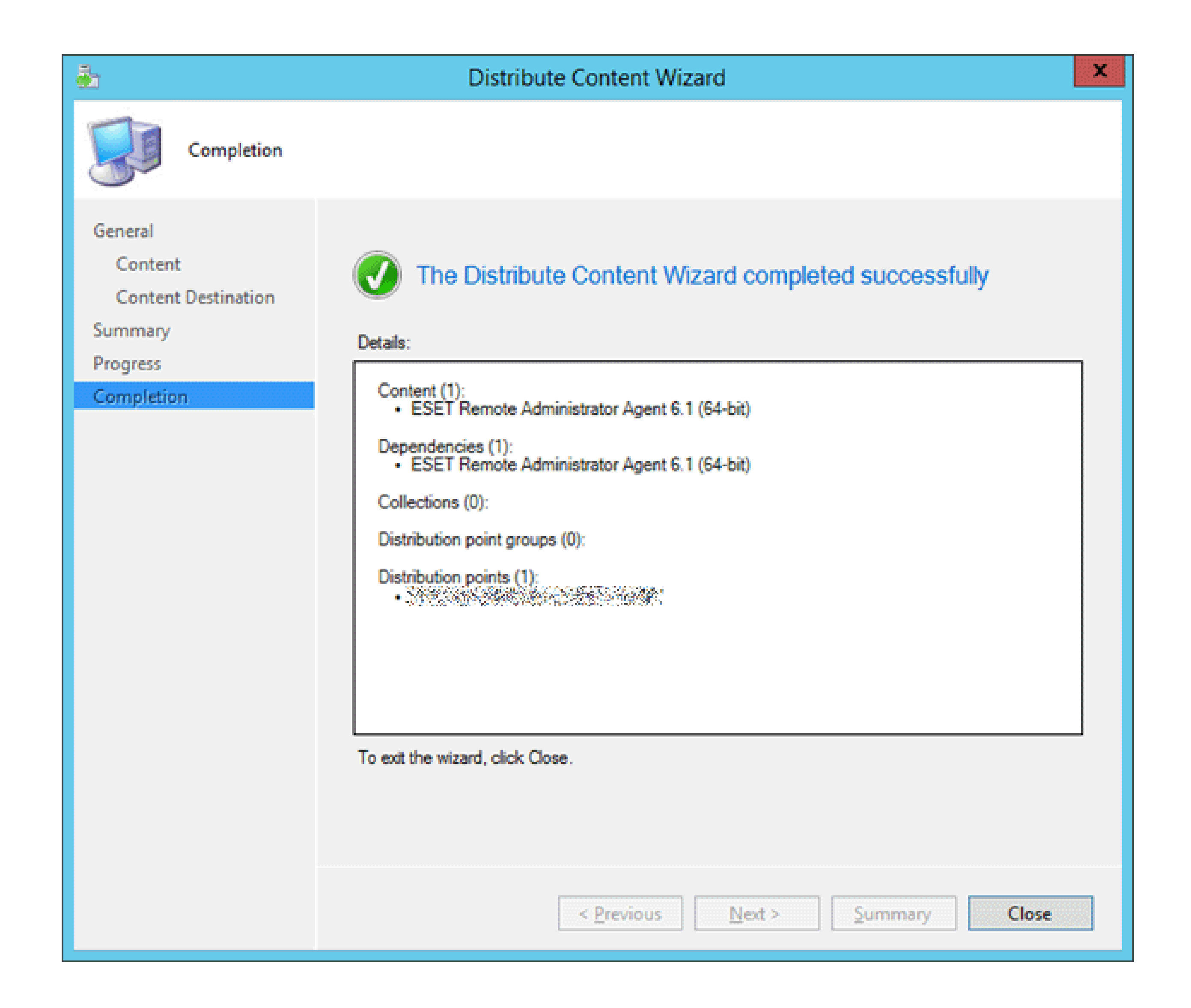
Filter...

Add

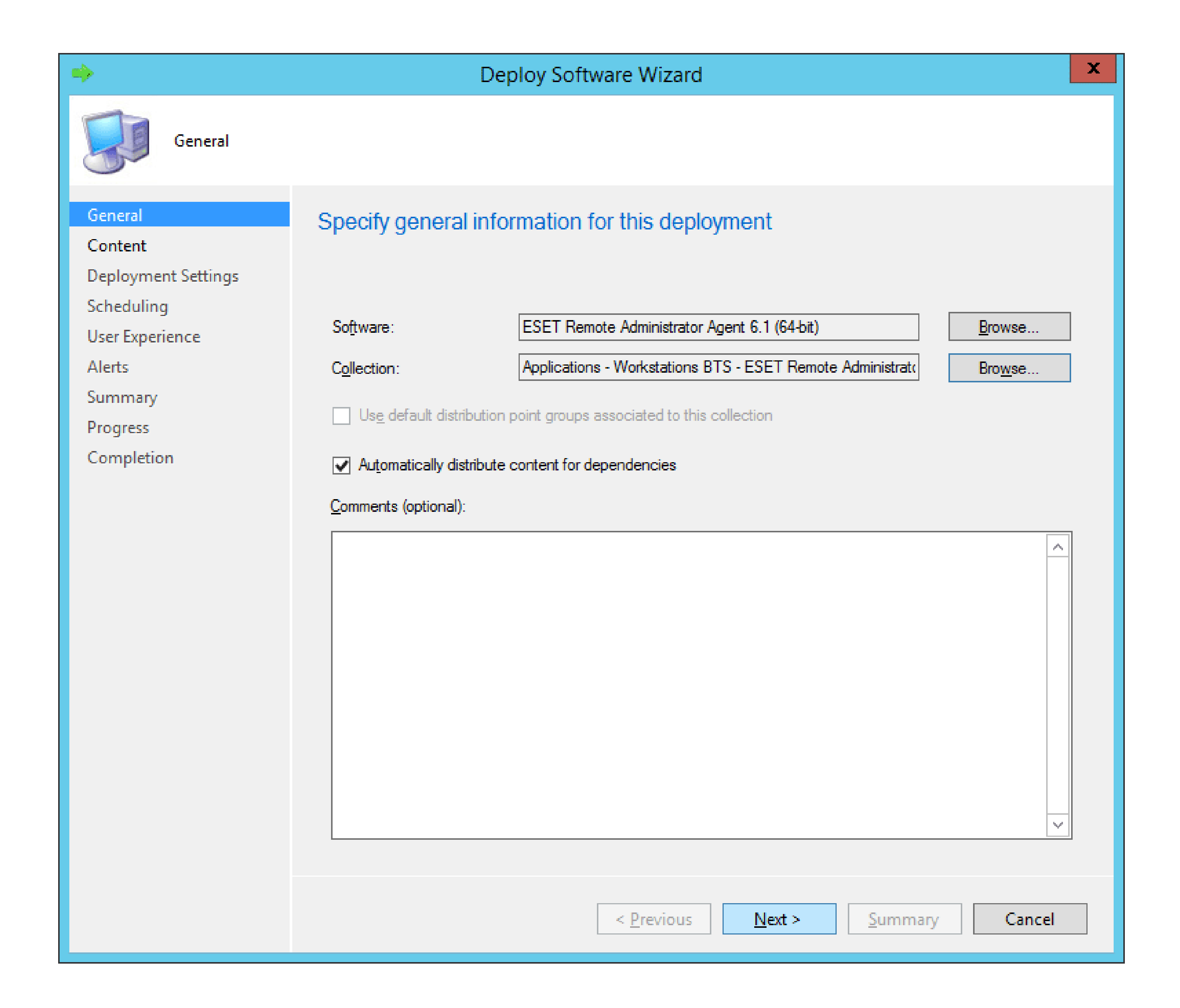
Remove

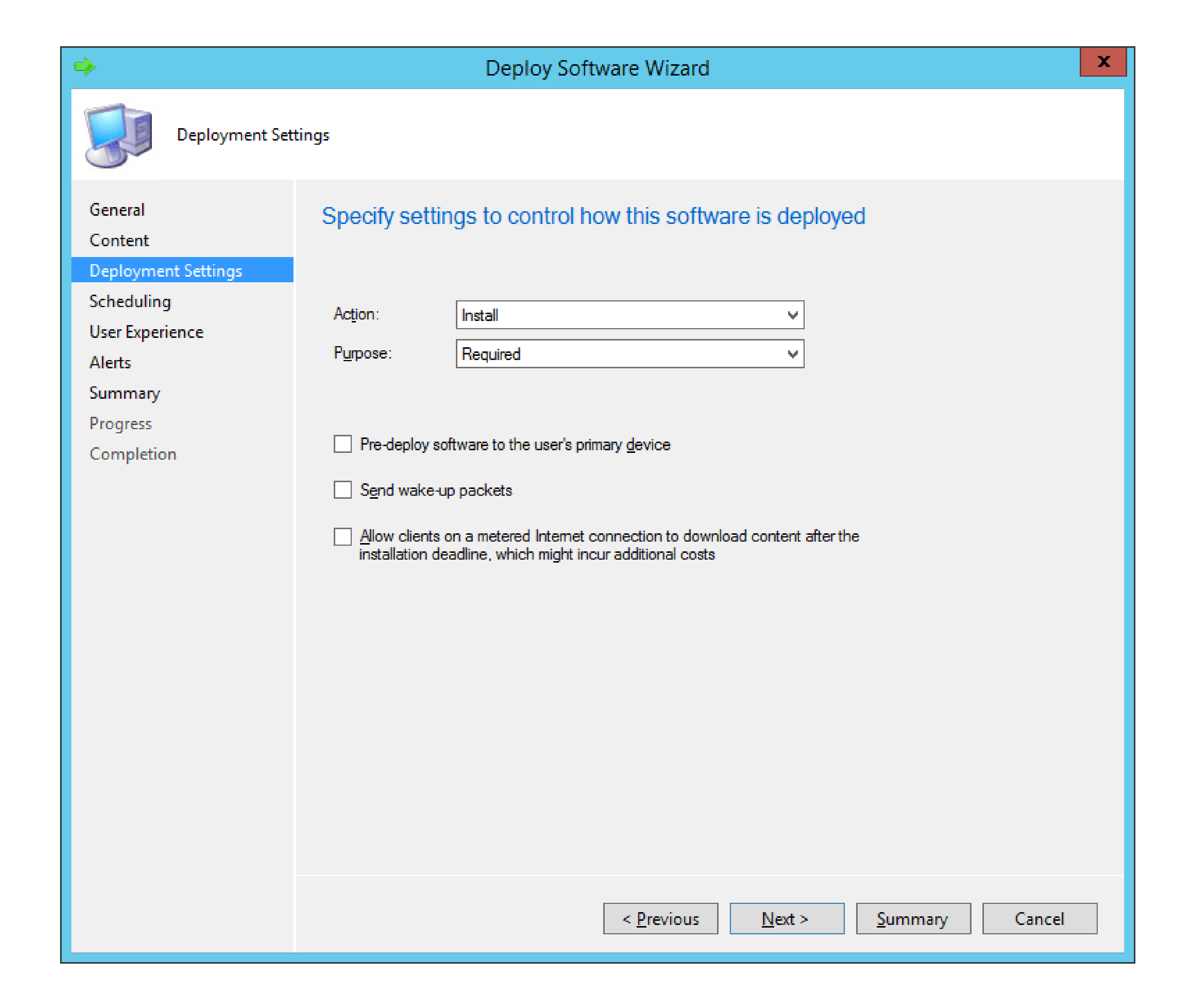
Name	Description	Associations
	Distribution point	

< Previous | Next > | Summary | Cancel

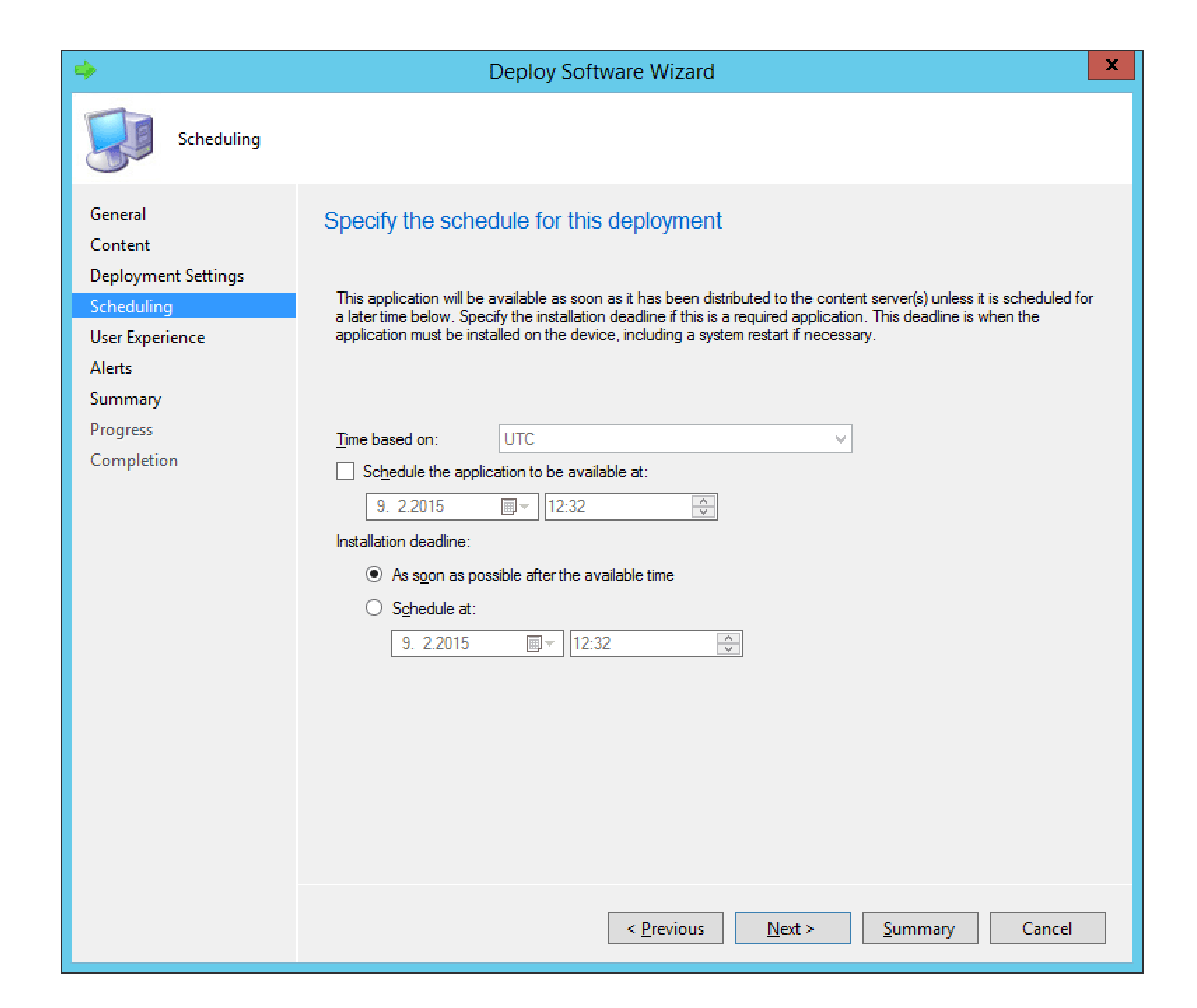


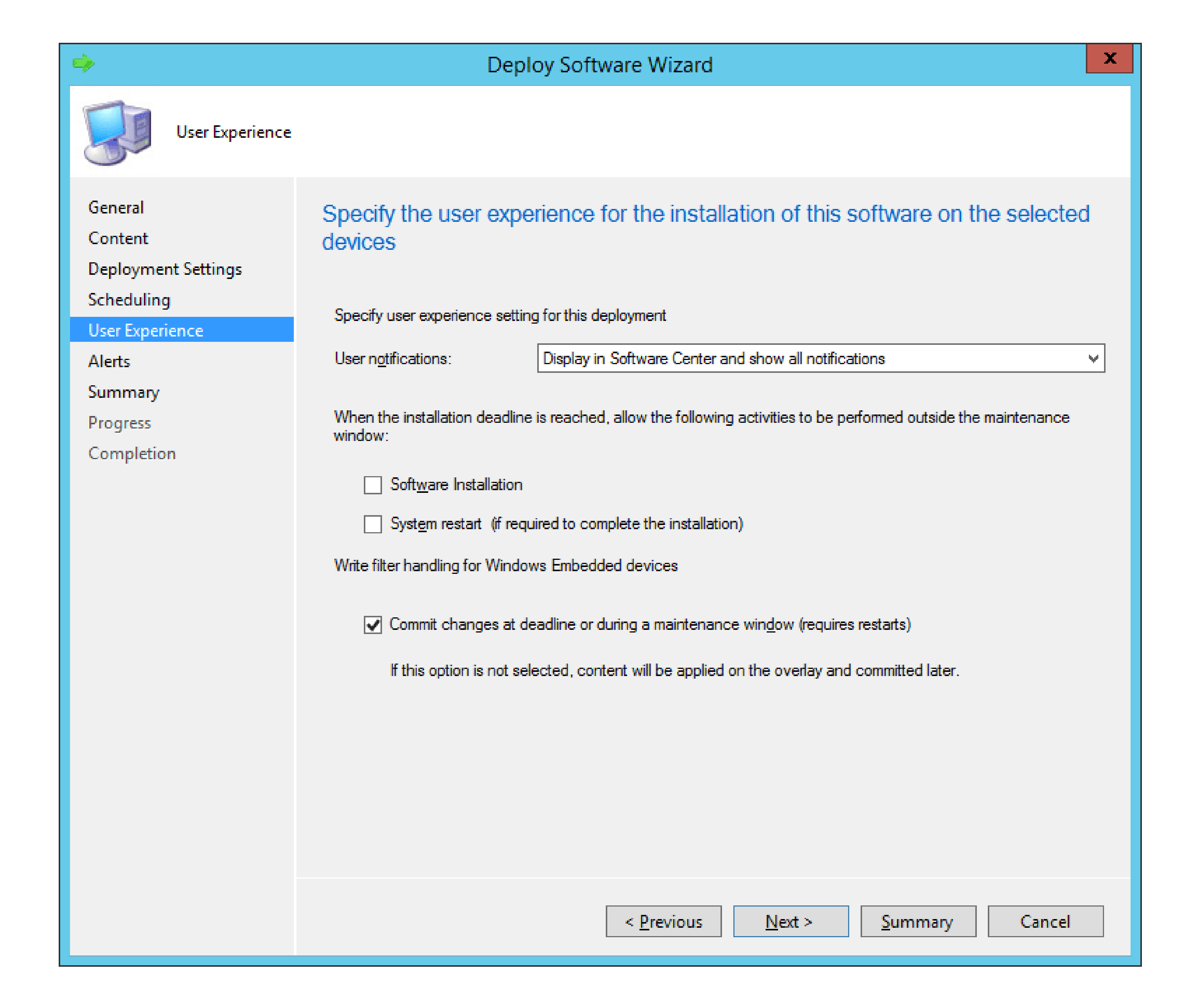
Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent 6.1 (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

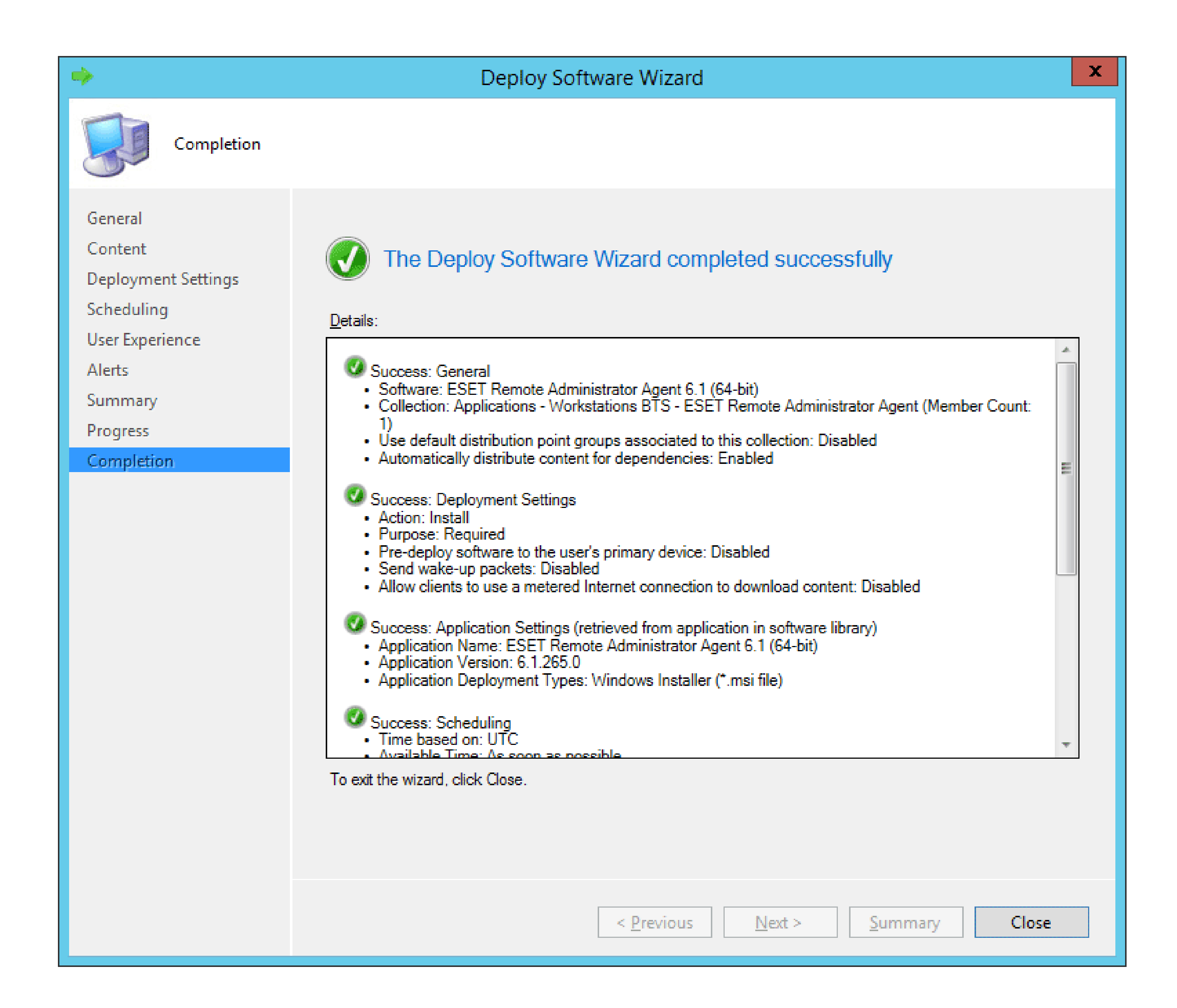

Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent 6.1 (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrato
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel



Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel

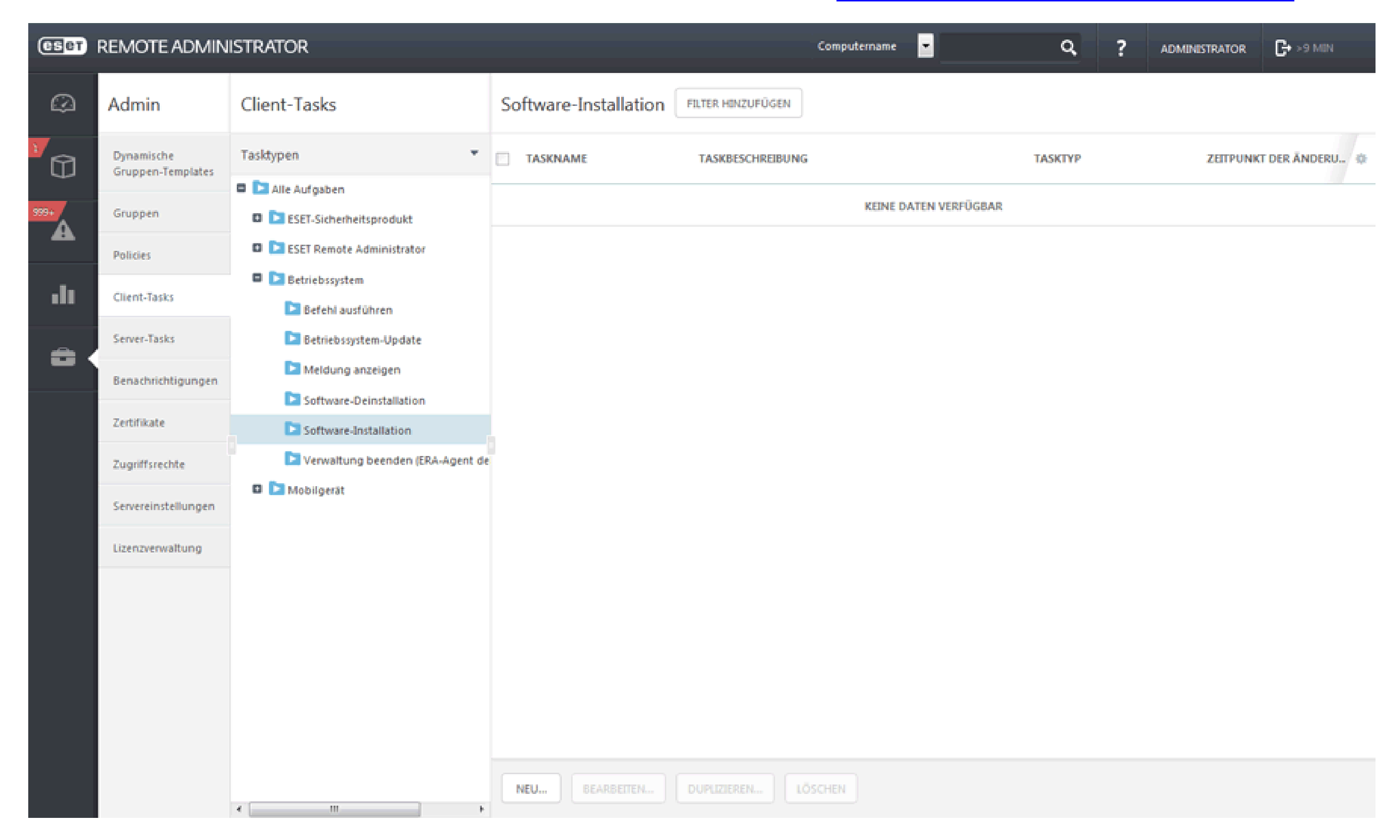

Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Completion
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
The Deploy Software Wizard completed successfully
Details:
Success: General
• Software: ESET Remote Administrator Agent 6.1 (64-bit)
• Collection: Applications - Workstations BTS - ESET Remote Administrator Agent (Member Count: 1)
• Use default distribution point groups associated to this collection: Disabled
• Automatically distribute content for dependencies: Enabled
Success: Deployment Settings
• Action: Install
• Purpose: Required
• Pre-deploy software to the user's primary device: Disabled
• Send wake-up packets: Disabled
• Allow clients to use a metered Internet connection to download content: Disabled
Success: Application Settings (retrieved from application in software library)
• Application Name: ESET Remote Administrator Agent 6.1 (64-bit)
• Application Version: 6.1.265.0
• Application Deployment Types: Windows Installer (*.msi file)
Success: Scheduling
• Time based on: UTC
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

4.4.4 Produktinstallation

ESET-Sicherheitsprodukte können remote installiert werden. Klicken Sie hierzu auf den gewünschten Computer und wählen Sie **Neu** aus oder erstellen Sie einen neuen Task **Software-Installation** im Menü **Admin** > **Client-Tasks**. Klicken Sie auf **Neu...**, um mit der Einrichtung des neuen Tasks zu beginnen.

- Führen Sie die folgenden Anweisungen aus oder sehen Sie sich das Anleitungsvideo in der Knowledgebase an.



Basis

Geben Sie grundlegende Informationen zum Task ein, wie **Name** und fakultativ eine **Beschreibung** und den **Tasktyp**. Der **Tasktyp** (siehe Liste oben) legt die Einstellungen und das Verhalten des Tasks fest. Wählen Sie den Task **Software-Installation** aus und klicken Sie dann auf **Ziel**.

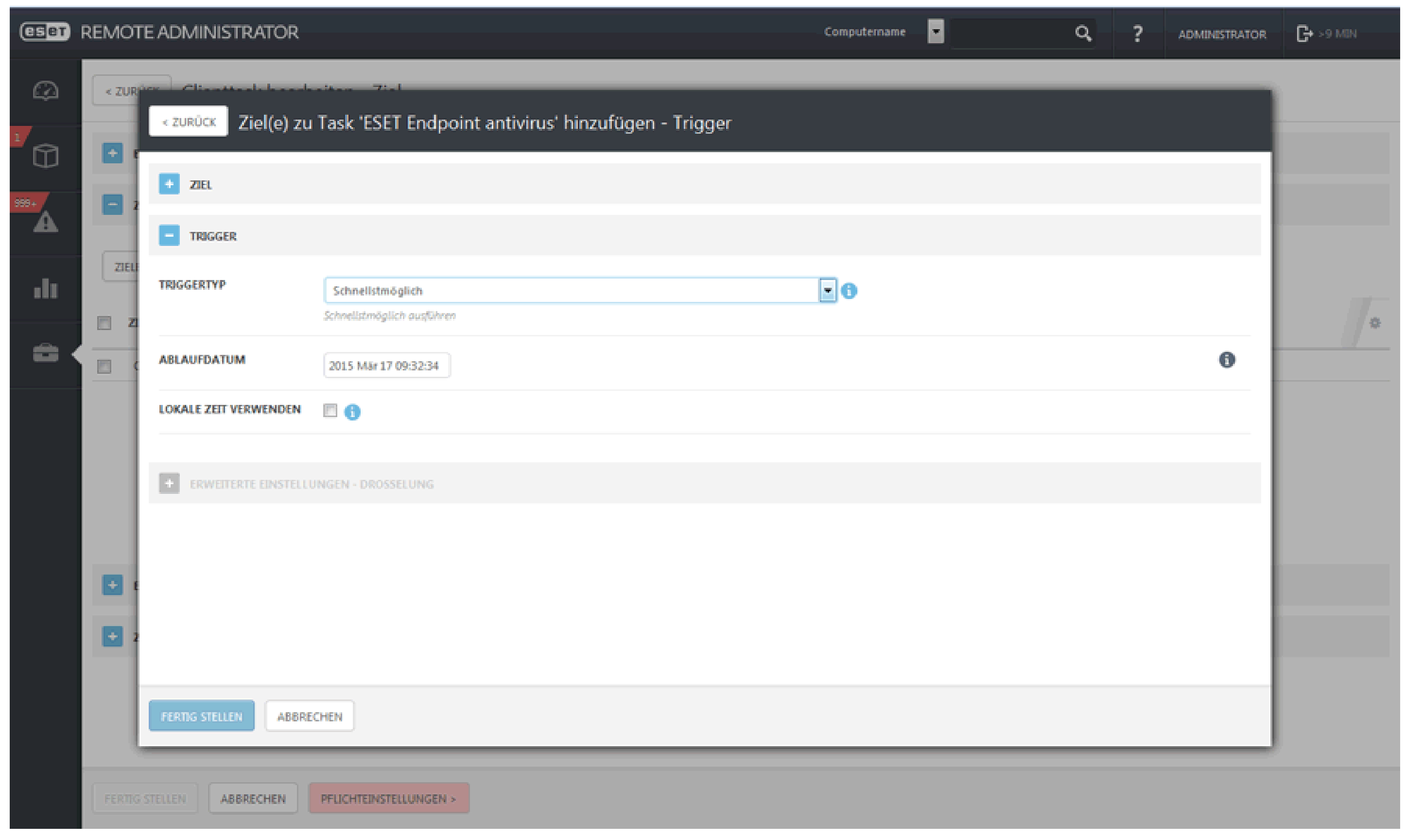
Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die den Task empfangen sollen.

Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.

Trigger

Als **Trigger** wählen Sie „Schnellstmöglich ausführen“ aus. Damit wird der Tasks sofort zu den Clients gesendet. Die Option **Lokale Zeit verwenden** bezieht sich auf die lokale Zeit auf dem Clientsystem, nicht auf dem Server.



Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Trigger bei Aufnahme in dynamische Gruppe** (siehe oben). Lassen Sie die Option Drosselung zunächst unverändert. Klicken Sie auf „Fertig stellen“, um den neuen Task zu erstellen.

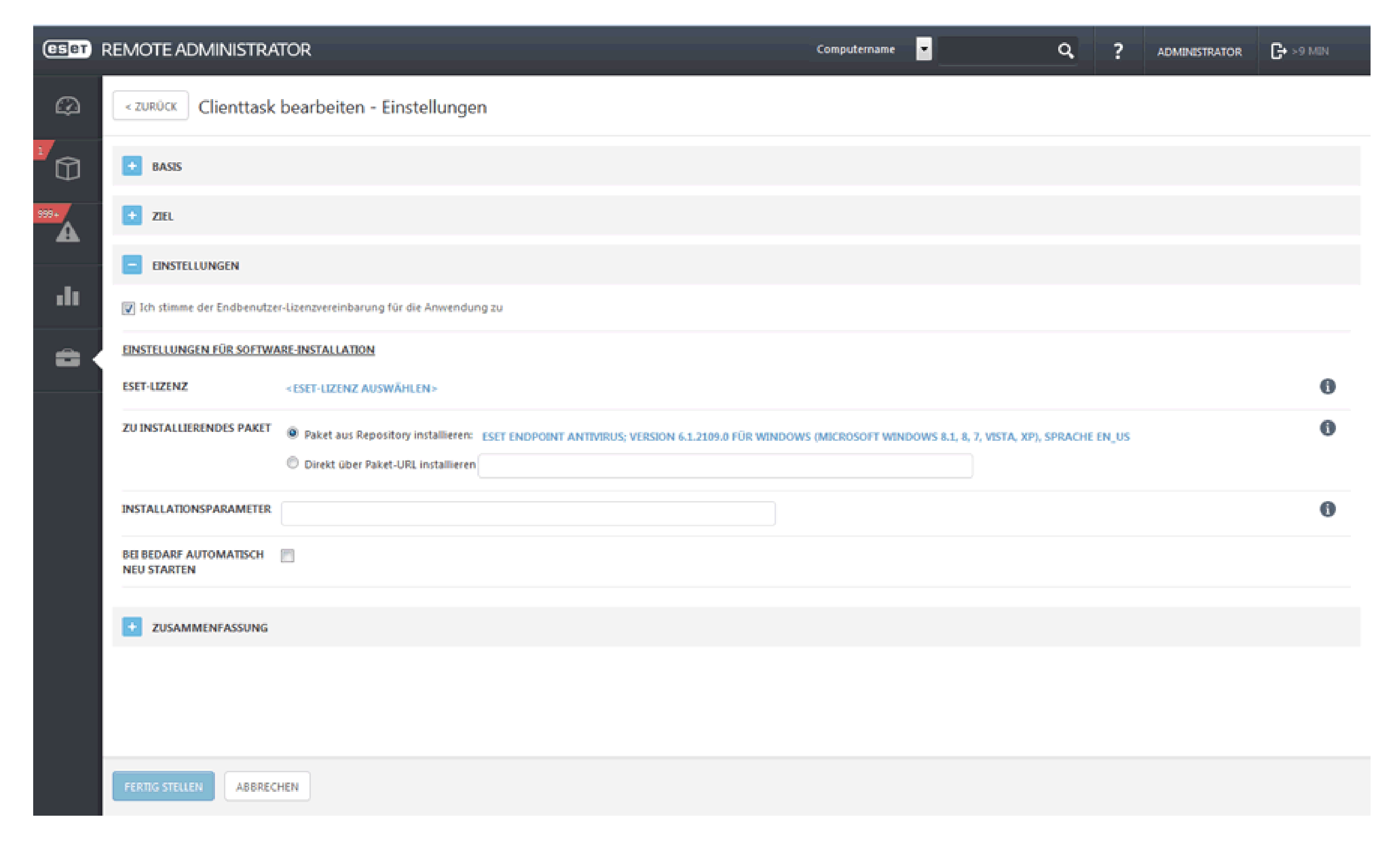
Einstellungen

Klicken Sie auf **<ESET-Lizenz auswählen>** und wählen Sie aus der Liste der verfügbaren Lizenzen die geeignete Lizenz für das installierte Produkt aus. Aktivieren Sie das Kontrollkästchen neben **Ich stimme der Endbenutzer-Lizenzvereinbarung für die Anwendung zu**, sofern Sie zustimmen. Weitere Informationen hierzu finden Sie unter Lizenzverwaltung oder EULA.

Klicken Sie auf **<Paket auswählen>**, um ein Installationspaket aus dem Repository auszuwählen, oder geben Sie eine Paket-URL ein. Eine Liste verfügbarer Pakete wird angezeigt, in der Sie das zu installierende ESET-Produkt (zum Beispiel ESET Endpoint Security) auswählen können. Wählen Sie das gewünschte Installationspaket aus und klicken Sie auf **OK**. Wenn Sie eine URL für das Installationspaket angeben möchten, geben Sie die URL durch Eintippen oder Kopieren und Einfügen in das Textfeld ein (verwenden Sie keine URLs, die Authentifizierung erfordern).

HINWEIS: Beachten Sie, dass Server und Agent mit dem Internet verbunden sein müssen, um auf das Repository zugreifen und die Installation durchführen zu können. Falls Sie keinen Internetzugriff haben, können Sie die Clientsoftware lokal installieren.

Bei Bedarf können Sie Installationsparameter angeben. Andernfalls lassen Sie dieses Feld leer. Aktivieren Sie das Kontrollkästchen neben Bei Bedarf automatisch neu starten, um einen automatischen Neustart des Computers nach der Installation zu erzwingen. Sie können diese Option auch deaktiviert lassen. Die Entscheidung über den Neustart wird dann vom Benutzer des Clientcomputers getroffen.



Zusammenfassung

Überprüfen Sie die Zusammenfassung der konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**. Der Task ist jetzt erstellt und wird an den/die Client(s) gesendet.

4.4.4.1 Produktinstallation (Befehlszeile)

Die folgenden Einstellungen sind nur mit den Einstellungen **reduziert**, **einfach und keine** der Benutzeroberfläche geeignet. Informationen zur msiexec-Version für die Befehlszeilenschalter finden Sie in der Dokumentation.

APPDIR="<path>"

- path – gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendung.

APPDATADIR="<path>"

- path – gültiger Verzeichnispfad
- Installationsverzeichnis der Anwendungsdaten.

MODULEDIR="<path>"

- path – gültiger Verzeichnispfad
- Installationsverzeichnis des Moduls.

ADDLOCAL="<list>"

- Komponenteninstallation – Liste nicht obligatorischer Funktionen, die lokal installiert werden sollen.
- siehe http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
- 0 – deaktiviert, 1 – aktiviert
- Eventuell unerwünschte Anwendungen

CFG_LIVEGRID_ENABLED=1/0
• 0 – deaktiviert, 1 – aktiviert
• LiveGrid

CFG_REPORTING_ENABLED=1/0
• 0 – deaktiviert, 1 – aktiviert
• Anonyme Nutzungsdaten aus LiveGrid

CFG_PCU_UPDATE_MODE=40/36/34
• 34 – fragen, 36 – immer, 40 – nie
• Modus des Programmkomponenten-Updates.

CFG_FIRSTSCAN_ENABLE=1/0
• 0 – deaktiviert, 1 – aktiviert
• Planen Sie einen neuen „FirstScan“ nach der Installation.

CFG_EPFW_MODE=0/1/2/3
• 0 – automatisch, 1 – interaktiv, 2 – Policy, 3 – Lernen

CFG_PROXY_ENABLED=0/1
• 0 – deaktiviert, 1 – aktiviert

CFG_PROXY_ADDRESS=<IP>
• IP-Adresse des Proxyservers.

CFG_PROXY_PORT=<Port>
• Proxy-Portnummer.

CFG_PROXY_USERNAME="<Benutzer>"
• Benutzername für die Authentifizierung.

CFG_PROXY_PASSWORD="<Passwort>"
• Passwort für die Authentifizierung.

4.4.4.2 Liste der Probleme bei Installationsfehlern

- Installationspaket nicht gefunden.
- Neuere Version des Windows Installer-Dienstes wird benötigt.
- Eine andere Version oder ein in Konflikt stehendes Produkt ist bereits installiert.
- Eine andere Installation wird bereits ausgeführt. Schließen Sie die andere Installation ab, bevor Sie diese Installation fortsetzen.
- Installation bzw. Deinstallation erfolgreich, allerdings ist ein Computerneustart erforderlich.
- Task fehlgeschlagen: Es ist ein Fehler aufgetreten. Überprüfen Sie den Trace-Log des Agenten und den Rückgabecode des Installationsprogramms.

4.5 Verwaltung

Dieser Abschnitt beschreibt das Hinzufügen von Computern oder Mobilgeräten zu Gruppen. Außerdem wird beschrieben, wie eine neue Policy erstellt und einer Gruppe zugewiesen wird.

4.5.1 Hinzufügen von Computern zu Gruppen

Clientcomputer können zu Gruppen hinzugefügt werden. Mithilfe der Gruppen können Sie die Computer je nach Bedarf anordnen und sortieren. Sie können Computer zu statischen oder dynamischen Gruppen hinzufügen.

Statische Gruppen werden manuell verwaltet. Dynamische Gruppen hingegen werden automatisch auf Grundlage bestimmter Kriterien erstellt, die in einem Template definiert werden. Nachdem Sie Computer zu den Gruppen hinzugefügt haben, können Sie den Gruppen Policies, Tasks oder Einstellungen zuweisen. Die Policy, der Task bzw. die Einstellung wird dann auf alle Mitglieder der Gruppe angewendet. Zwischen Gruppen und Tasks/Policies gilt folgende Beziehung:

Statische Gruppen

Statische Gruppen sind Gruppen manuell ausgewählter und konfigurierter Clients. Die Mitglieder sind statisch und können nur manuell und nicht auf Grundlage dynamischer Kriterien hinzugefügt/entfernt werden.

Dynamische Gruppen

Dynamische Gruppen sind Gruppen aus Clients, deren Mitgliedschaft in der Gruppe nach bestimmten Kriterien festgelegt wird. Wenn ein Client die Kriterien nicht erfüllt, wird er aus der Gruppe entfernt. Computer, die die Kriterien erfüllen, werden automatisch zur Gruppe hinzugefügt. Die Gruppe wird also „dynamisch“ erstellt.

4.5.1.1 Statische Gruppen

- Statische Gruppen dienen dem manuellen Ordnen der Clientcomputer in **Gruppen** und **Untergruppen**. Sie können benutzerdefinierte statische Gruppen erstellen und die gewünschten Computer in diese Gruppen verschieben.
- Statische Gruppen können nur manuell erstellt werden. Anschließend können Clientcomputer manuell in diese Gruppen verschoben werden. Jeder Computer kann stets nur zu einer statischen Gruppe gehören.

Es gibt zwei standardmäßige statische Gruppen:

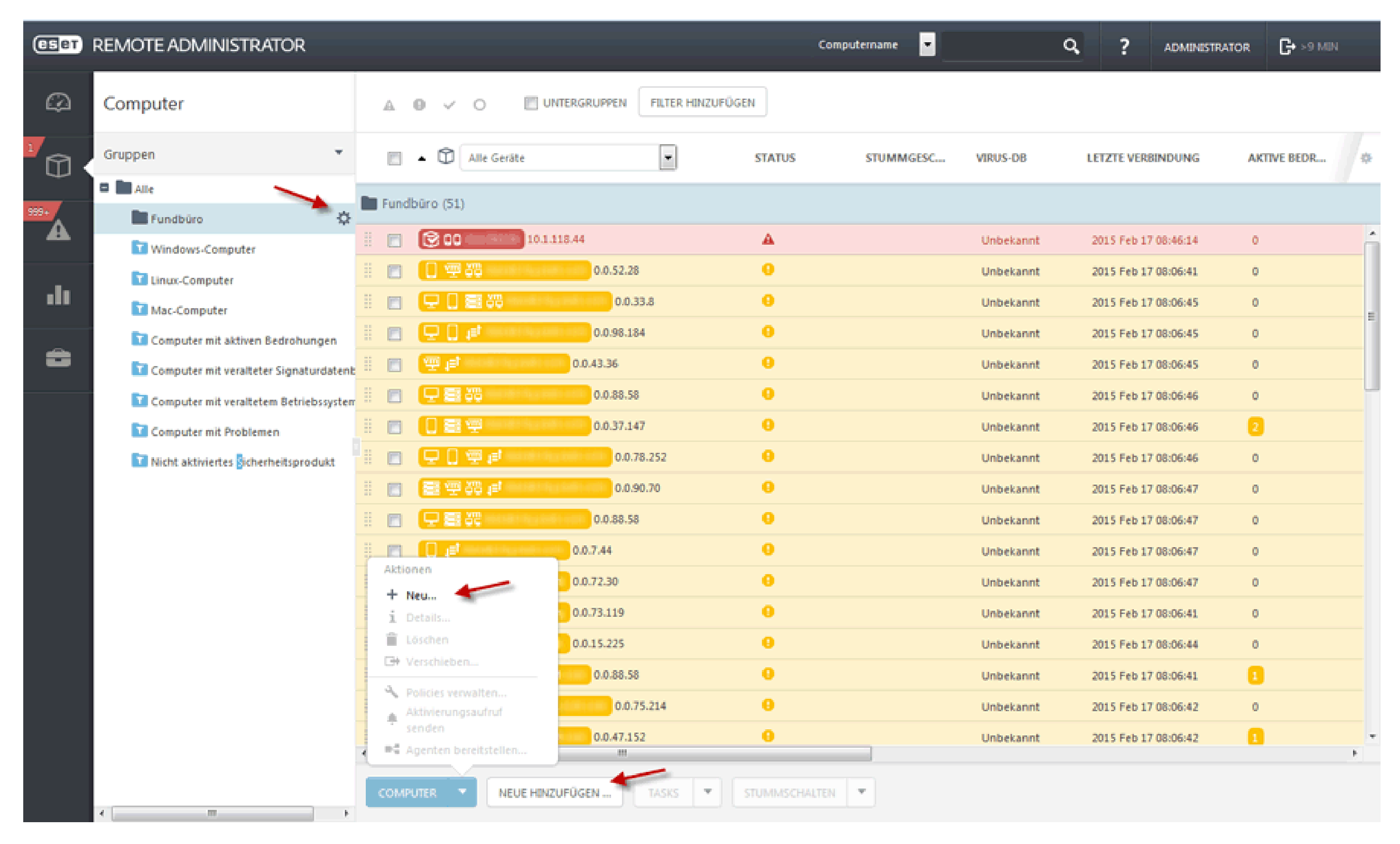
- **Alle –** Dies ist eine Hauptgruppe für alle Computer im Netzwerk des ERA-Servers. Über diese Gruppe werden die Policies auf jeden Computer als standardmäßige Policy angewendet. Die Gruppe wird immer angezeigt und ihr Name kann nicht geändert werden.
- **Fundbüro** als Untergruppe der Gruppe **Alle** – Bei der ersten Verbindung zwischen Agent und Server wird jeder neue Computer zunächst automatisch in dieser Liste angezeigt. Die Gruppe kann umbenannt und kopiert werden, jedoch nicht gelöscht oder verschoben.

Klicken Sie zum Erstellen statischer Gruppen im Bereich **Gruppen** der Registerkarte **Admin** auf die Schaltfläche Gruppen und wählen Sie Neue statische Gruppe aus.

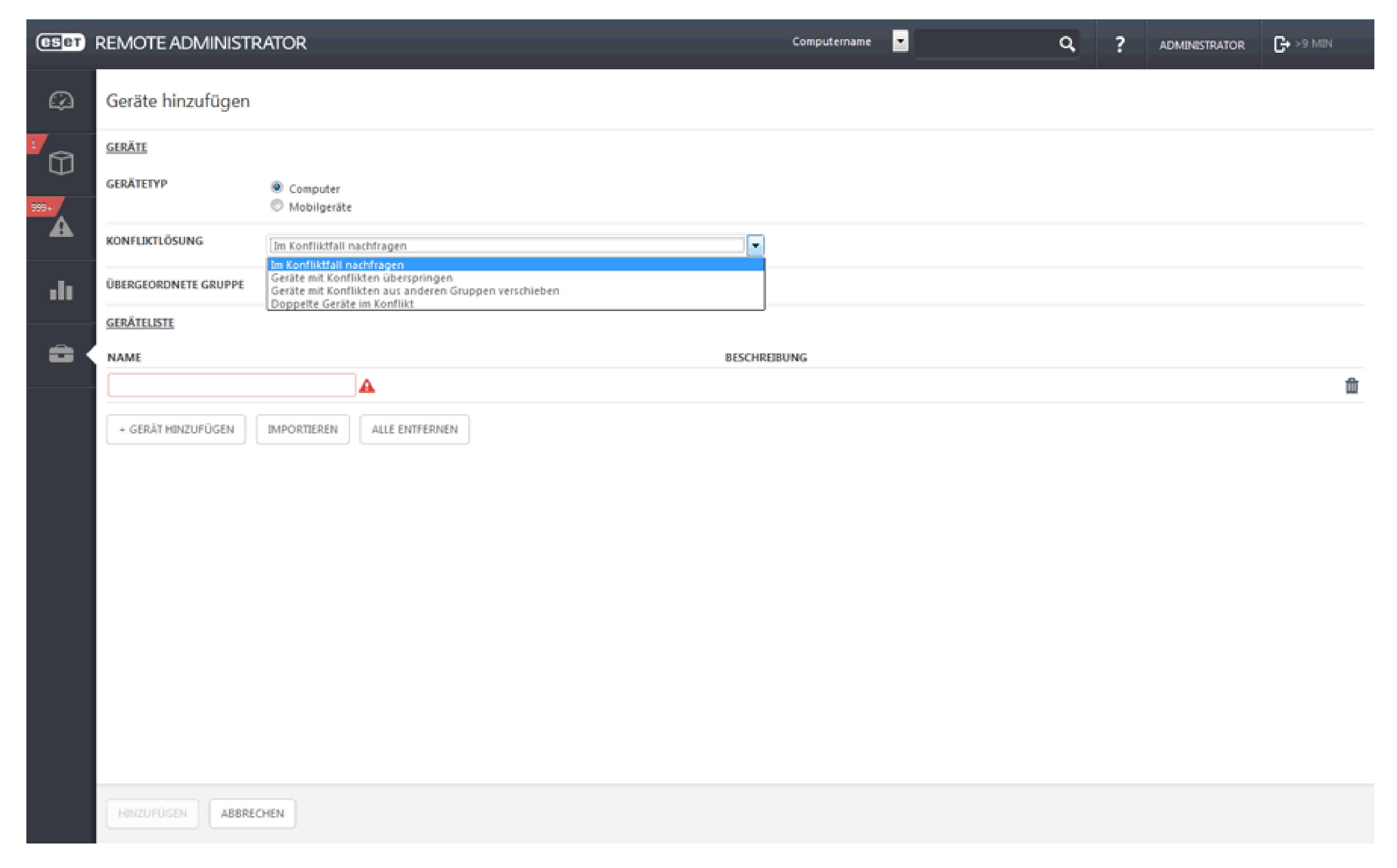
4.5.1.1.1 Hinzufügen eines Computers zu einer statischen Gruppe

Erstellen Sie eine neue statische Gruppe oder wählen Sie eine der standardmäßigen statischen Gruppen aus.

Die **Registerkarte** Computer bietet drei Möglichkeiten zum Hinzufügen neuer Computer. Wählen Sie beispielsweise eine statische Gruppe aus, klicken Sie auf das Zahnradsymbol ⚙ und wählen Sie **+ Neue hinzufügen** aus.



Geben Sie den Namen des hinzuzufügenden Computers in das Feld **Name** ein. Klicken Sie auf + Gerät hinzufügen, um zusätzliche Computer hinzuzufügen, oder klicken Sie auf Importieren, um eine Datei mit einer Liste der hinzuzufügenden Computer zu importieren. Wahlweise können Sie eine **Beschreibung** für die Computer eingeben.



Im Dropdown-Menü „Konfliktlösung“ können Sie eine Aktion für den Fall auswählen, dass der Computer bereits in ERA vorhanden ist:

Im Konfliktfall nachfragen: Wenn ein Konflikt erkannt wird, fordert das Programm Sie zur Auswahl einer Aktion auf (siehe nachstehende Optionen).
Computer mit Konflikten überspringen: Bereits vorhandene Computer werden nicht hinzugefügt.
Computer mit Konflikten aus anderen Gruppen verschieben: Computer mit Konflikten werden aus der ursprünglichen Gruppe in die Gruppe **Alle** verschoben.
Computer mit Konflikten duplizieren: Neue Computer werden hinzugefügt, jedoch mit einem anderen Namen.

Klicken Sie auf **Hinzufügen**. Wenn Sie eine Gruppe auswählen, werden rechts in der Liste die zur Gruppe gehörenden Computer angezeigt.

HINWEIS: Das Hinzufügen mehrerer Computer kann einige Zeit in Anspruch nehmen, Reverse-DNS-Lookup kann durchgeführt werden.

Weitere Informationen zum Hinzufügen von Mobilgeräten finden Sie im Kapitel Mobilgeräteregistrierung.

4.5.1.2 Dynamische Gruppen

In jeder dynamischen Gruppe wird ein Template verwendet, um die Clientcomputer zu filtern. Ein einmal definiertes Template kann später in anderen dynamischen Gruppen zum Filtern der Clients verwendet werden. ERA enthält mehrere einsatzbereite standardmäßige Templates für dynamische Gruppen, mit denen Sie die Clientcomputer auf einfache Weise in Kategorien gliedern können.

Dynamische Gruppen sind Gruppen von Clients, die auf Grundlage bestimmter Kriterien ausgewählt werden. Wenn ein Clientcomputer die Kriterien nicht erfüllt, wird er aus der Gruppe entfernt. Wenn der Computer die festgelegten Bedingungen erfüllt, wird er zur Gruppe hinzugefügt. Die Auswahl der Gruppenmitglieder erfolgt automatisch auf Grundlage der konfigurierten Einstellungen. Bei statischen Gruppen ist dies jedoch nicht der Fall.

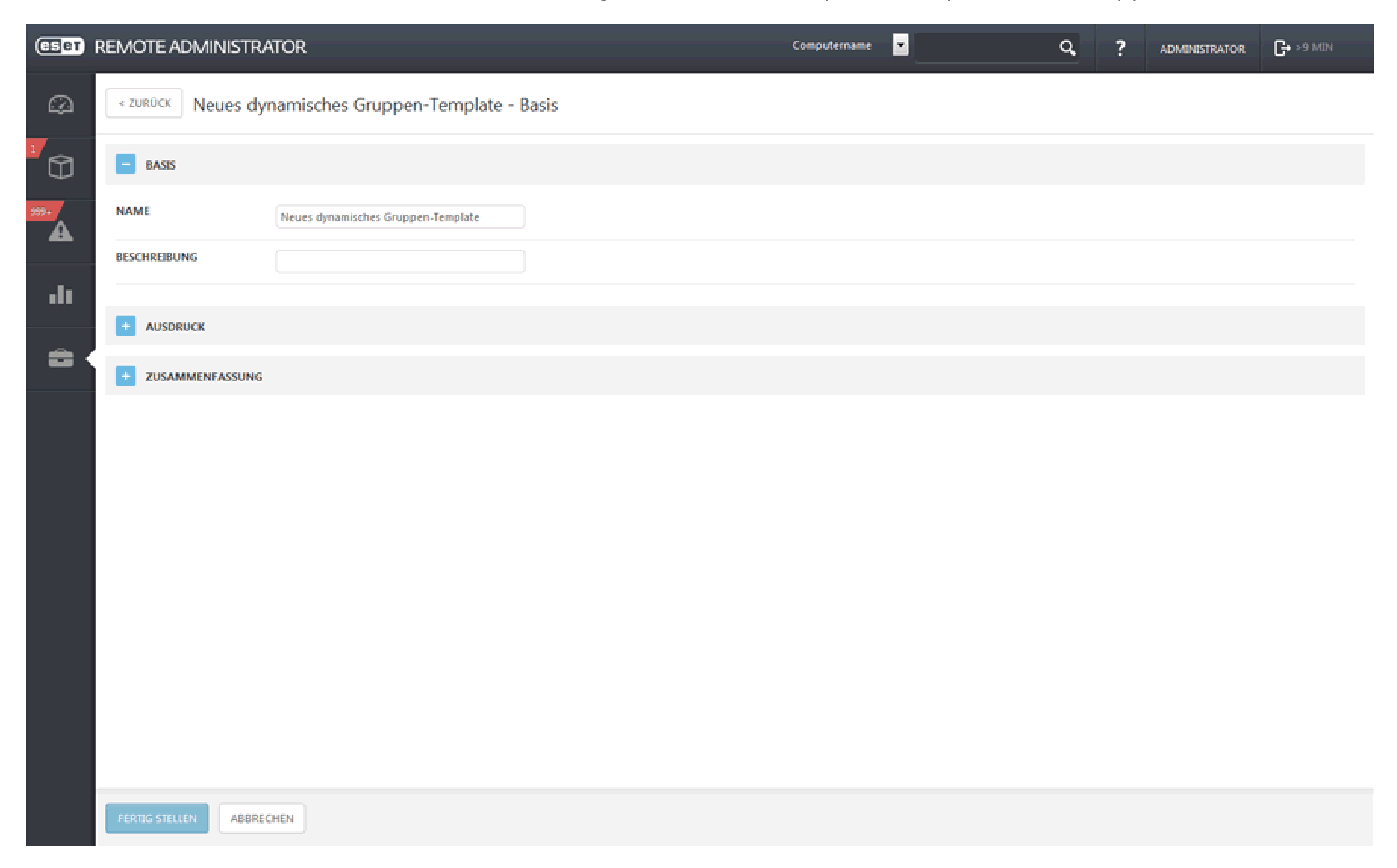
Im Abschnitt der Templates für dynamische Gruppen sind vordefinierte und benutzerdefinierte Templates enthalten, die auf unterschiedlichen Kriterien basieren. Alle Templates werden in einer Liste angezeigt. Klicken Sie auf ein vorhandenes Template, um es zu bearbeiten. Um ein neues Template für eine dynamische Gruppe zu erstellen, klicken Sie auf **Neues Template**.

4.5.1.2.1 Neues Template für dynamische Gruppen

Klicken Sie auf **Neues Template** unter **Admin** > **Templates für dynamische Gruppen**.

Basis

1. Geben Sie einen **Namen** und eine **Beschreibung** für das neue Template für dynamische Gruppen ein.



Ausdruck

Wählen Sie einen logischen Operator im Menü **Operation** aus.

- **AND** – Alle festgelegten Bedingungen müssen erfüllt sein.
- **OR** – Mindestens eine Bedingung muss erfüllt sein.
- **NAND** – Mindestens eine Bedingung darf nicht erfüllt sein.
- **NOR** – Alle Bedingungen müssen falsch sein.

Wählen Sie beispielsweise **UND**. Dies bedeutet, dass der Computer alle Bedingungen erfüllen muss, um in der dynamischen Gruppe angezeigt zu werden, die dieses Template verwendet.

- Klicken Sie auf **+ Regel hinzufügen** und wählen Sie eine Bedingung aus. Nehmen wir an, Sie möchten Clients auswählen, die ein Notebook mit angeschlossenem Netzkabel verwenden. Wählen Sie **Hardware** > **Im Akkubetrieb** > **=(gleich)** > **Wird nicht entladen** aus.
- Klicken Sie auf **+ Regel hinzufügen**, um eine zweite Bedingung einzugeben (die Anzahl der Regeln ist unbegrenzt).Wählen Sie **Betriebssystemedition** > **OS-Typ** > **=(gleich)** > **Windows 8.1** (geben Sie diesen Wert in das leere Feld ein).

Wenn beide Bedingungen erfüllt sind, wird der Client in der dynamischen Gruppe angezeigt.

Zusammenfassung

Überprüfen Sie die konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**, um das neue Template zu erstellen. Das neue Template wird zur Liste der Templates hinzugefügt und kann später zum Erstellen einer neuen dynamischen Gruppe verwendet werden. Unter der Option **Ausdruck** können Sie Regeln/Bedingungen für die Gruppe konfigurieren (eine Beschreibung des Regel-Editors finden Sie hier). Jede auf diesem Template basierende dynamische Gruppe bewertet nun diese Regeln.

Klicken Sie zum Speichern Ihrer Änderungen auf **Fertig stellen**.

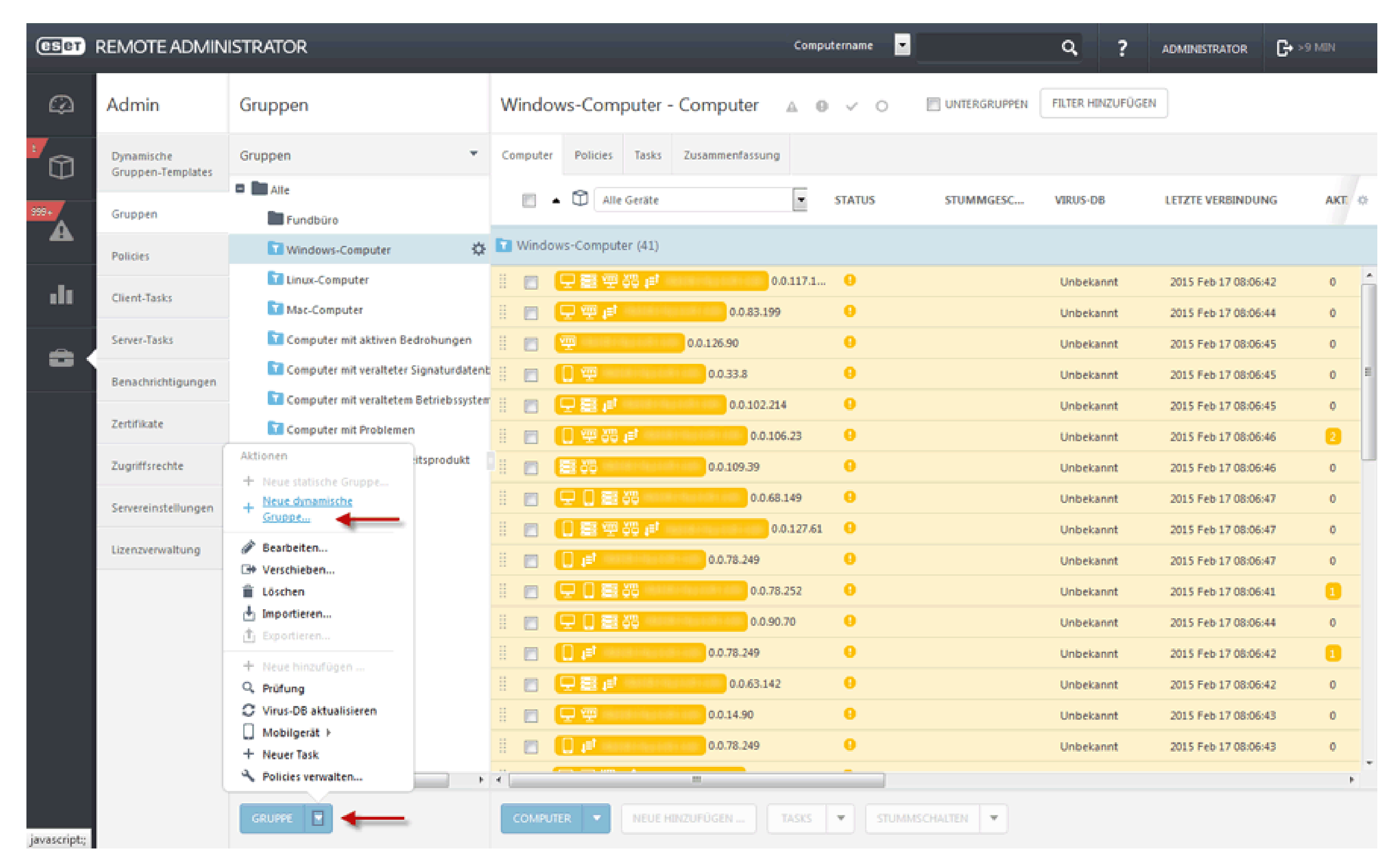
4.5.1.2.2 Erstellen einer neuen dynamischen Gruppe

Zum Erstellen einer neuen dynamischen Gruppe stehen drei Methoden zur Auswahl:

1. Klicken Sie auf **Computer** > **Gruppen** > ⚙ und anschließend auf **Neue dynamische Gruppe...**

2. Klicken Sie auf **Admin** > **Gruppen** > ⚙ > **Neue dynamische Untergruppe ....**

3. Klicken Sie auf **Admin** > **Gruppen**, klicken Sie anschließend auf die Schaltfläche **Gruppe** und auf **Neue dynamische Gruppe...**

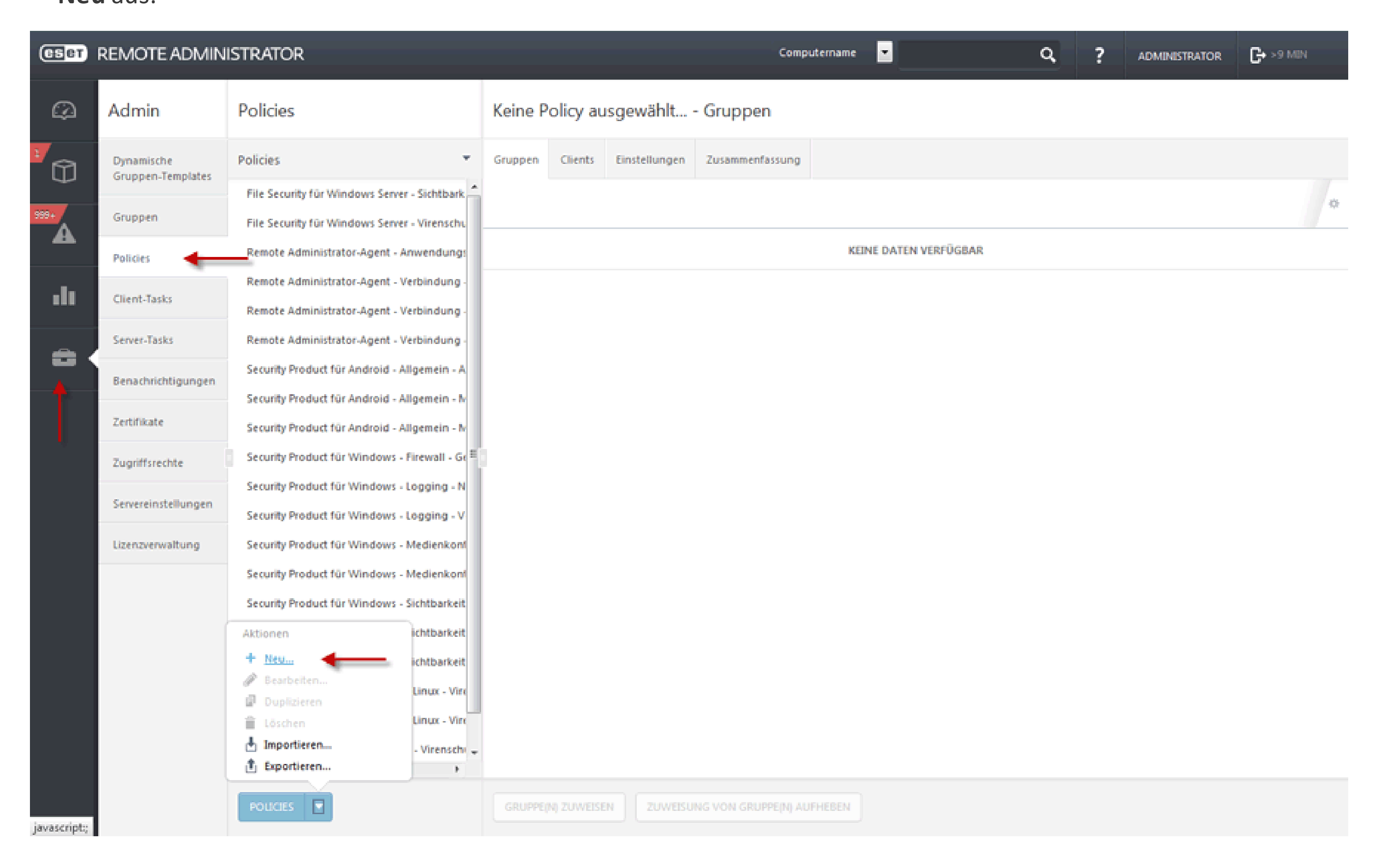


Der Assistent für neue dynamische Gruppen wird angezeigt.

4.5.2 Erstellen einer neuen Policy

In diesem Beispiel erstellen wir eine neue Policy für das Verbindungsintervall des ERA-Agenten. Testen Sie diesen Vorgang vor der massenhaften Bereitstellung unbedingt in Ihrer Umgebung.

1. Erstellen Sie eine Neue statische Gruppe.
2. Klicken Sie zum Erstellen einer neuen Policy auf **Admin** > **Policies**. Klicken Sie unten auf **Policies** und wählen Sie **Neu** aus.

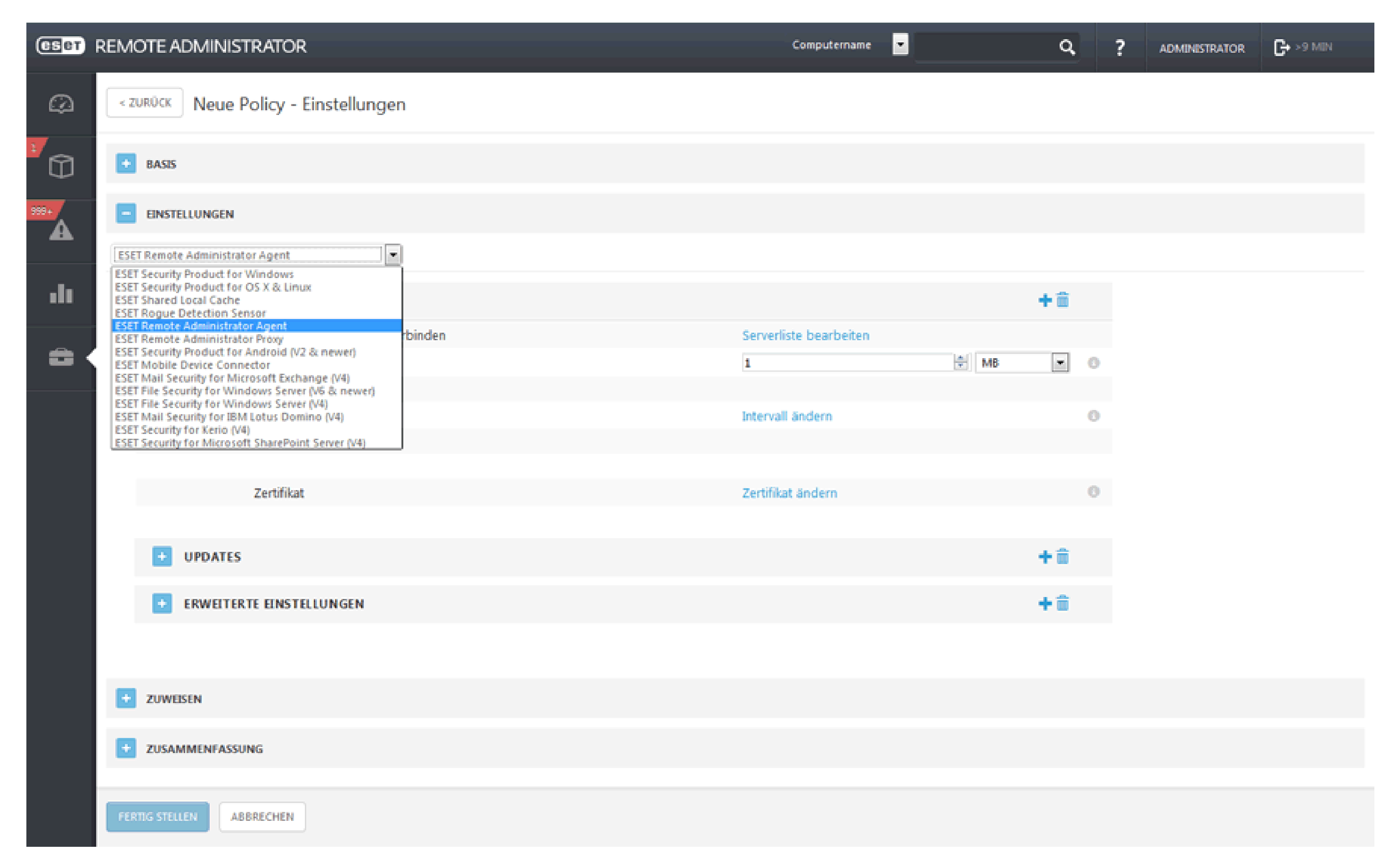


Basis

Geben Sie einen **Namen** für die neue Policy ein (zum Beispiel „Verbindungsintervall für Agent“). Die Eingabe in das Feld **Beschreibung** ist optional.

Einstellungen

Wählen Sie im Dropdownmenü **Produkt** den Eintrag **ESET Remote Administrator-Agent** aus.



Verbindung

Wählen Sie links in der Baumstruktur eine Kategorie aus. Bearbeiten Sie die Einstellungen auf der rechten Seite nach Bedarf. Jede Einstellung ist eine Regel, für die Sie eine Markierung festlegen können. Zur Vereinfachung der Navigation wird die Gesamtzahl aller Regeln berechnet. Die Anzahl aller in einem bestimmten Bereich definierten Regeln wird automatisch angezeigt. Außerdem wird neben den Kategorienamen links in der Baumstruktur eine weitere Zahl angezeigt. Dies ist die Summe der Regeln in den einzelnen Bereichen. Hier können Sie auf einen Blick sehen, wo und wie viele Einstellungen/Regeln definiert sind.

Mit den folgenden Empfehlungen können Sie die Bearbeitung von Policies vereinfachen:
- + verwenden, um die **Übernehmen**-Markierung für alle Elemente im aktuellen Bereich zu setzen
- Regeln mit dem **Papierkorb**-Symbol löschen

Klicken Sie auf **Intervall ändern**.

Ändern Sie den Wert im Feld **Reguläres Intervall** in den gewünschten Wert für die Intervalldauer (empfohlen: 60 Sekunden) und klicken Sie auf Speichern.

Sobald Sie eine neue Policy für das Agenten-Verbindungsintervall erstellt haben, weisen Sie es zu der statischen Gruppe zu, die Sie in Schritt 1 erstellt haben.

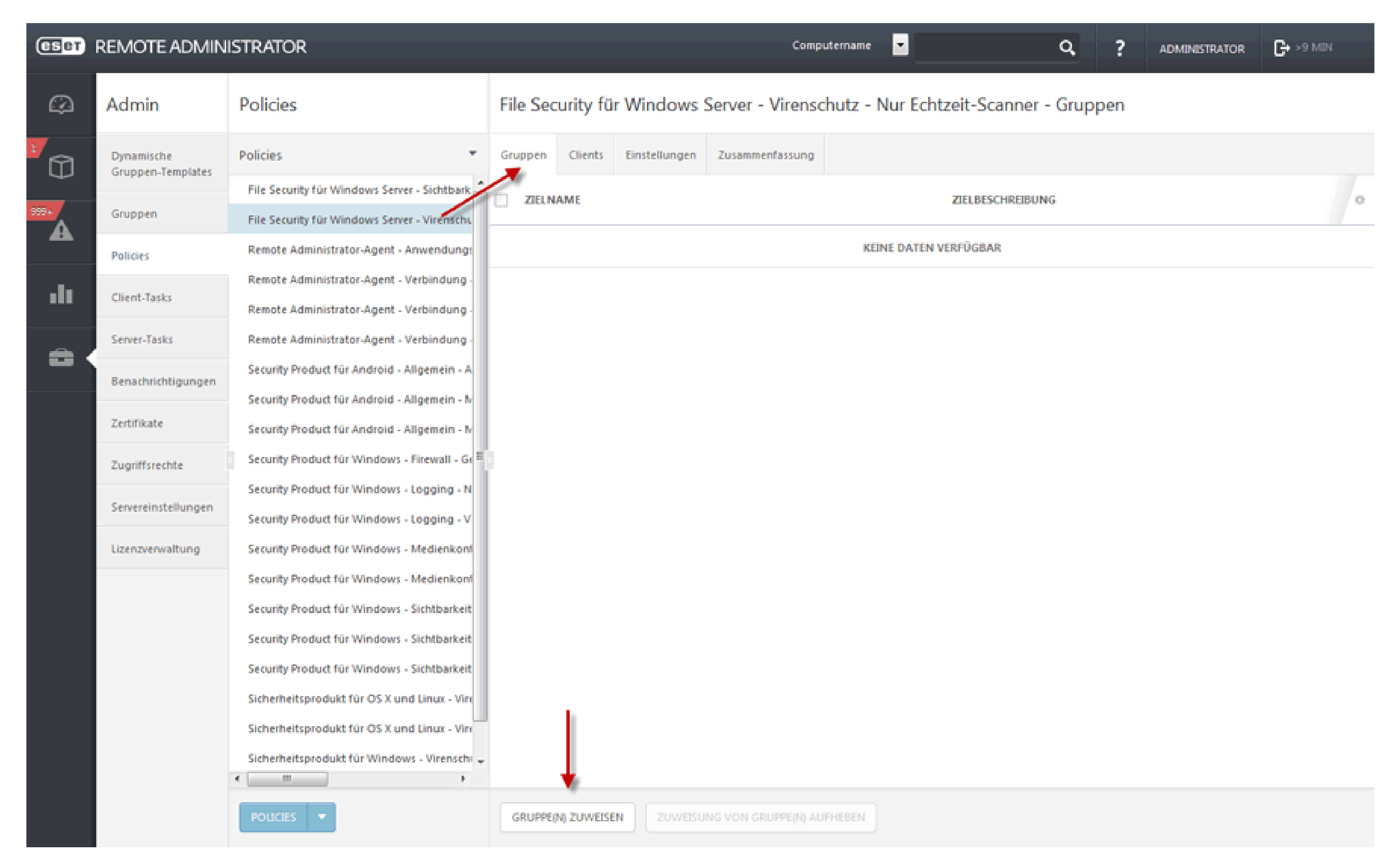
Führen Sie Ihre Tests für die massenhafte Bereitstellung durch und bearbeiten Sie anschließend die Einstellungen der Policy für das Agenten-Verbindungsintervall, das Sie in Schritt 2 erstellt haben.

Klicken Sie auf **Admin** > **Gruppen** und wählen Sie die Registerkarte **Policies** aus. Klicken Sie auf die Policy "Verbindungsintervall für Agent", wählen Sie **Bearbeiten** aus und klicken Sie auf **Einstellungen** > **Verbindung**. Klicken Sie auf **Intervall ändern** und setzen Sie das Verbindungsintervall auf 20 Minuten.

4.5.3 Zuweisen einer Policy zu einer Gruppe

Nachdem Sie eine Policy erstellt haben, können Sie sie einer **statischen** oder **dynamischen Gruppe** zuweisen. Es gibt zwei Möglichkeiten zum Zuweisen einer Policy:

1. Klicken Sie auf **Admin** > **Policies**, wählen Sie eine Policy aus und klicken Sie auf **Gruppe(n) zuweisen**. Wählen Sie eine statische oder dynamische Gruppe aus und klicken Sie auf **OK**.



Wählen Sie **Gruppe** in der Liste aus.

2. Klicken Sie auf **Admin** > **Gruppen** > **Gruppe** oder neben dem Gruppennamen auf das Zahnradsymbol ⚙. Wählen Sie **Policies** verwalten aus.

Klicken Sie im Fenster **Anwendungsreihenfolge für Policies** auf **Policy hinzufügen**. Aktivieren Sie das Kontrollkästchen neben der Policy, die Sie der Gruppe zuweisen möchten, und klicken Sie auf **OK**.
Klicken Sie auf **Speichern**. Um anzuzeigen, welche Policies einer bestimmten Gruppe zugewiesen sind, wählen Sie die gewünschte Gruppe aus und klicken Sie auf die Registerkarte **Policies**. Eine Liste der Policies, die dieser Gruppe zugewiesen sind, wird angezeigt.

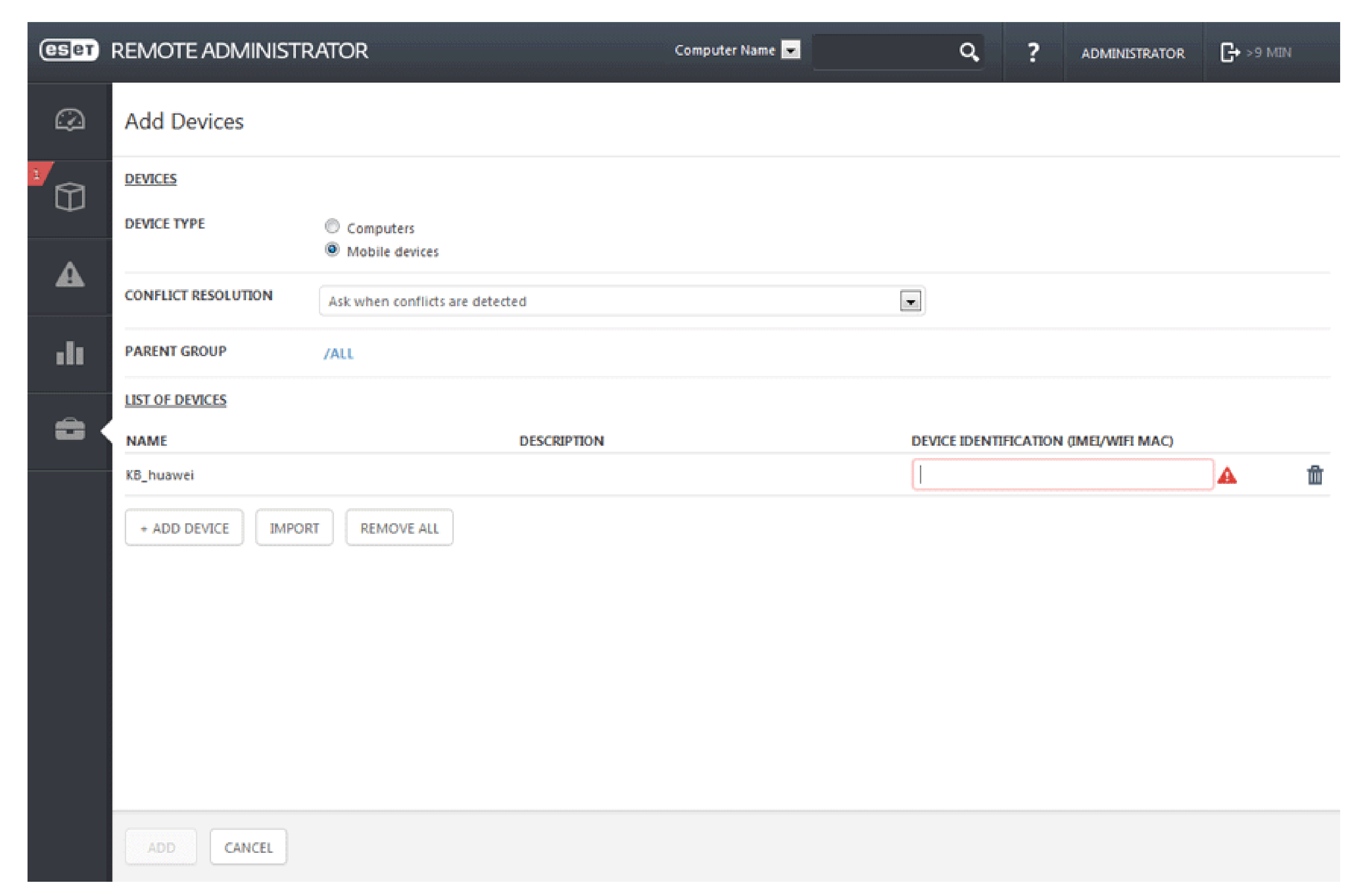
HINWEIS: Weitere Informationen zu Policies finden Sie im Kapitel Policies.

4.5.4 Mobilgeräteregistrierung

Sie können Mobilgeräte auf ähnliche Weise wie einen neuen Computer zur ERA-Struktur hinzufügen. Führen Sie dazu die folgenden Schritte aus:

1. Klicken Sie auf **Admin** > wählen Sie die statische Gruppe aus, zu der Sie das Mobilgerät hinzufügen möchten, und klicken Sie auf **Neu ....**

2. Wählen Sie die Option **Mobilgeräte** aus und geben Sie einen **Namen**, eine **Beschreibung** (optional) und die **Geräteidentifizierungsnummer** ein. Die Gerätedentifizierungsnummer ist entweder eine IMEI-Nummer (GSM-Netzwerke), eine MEID-Nummer (CDMA-Netzwerke) oder eine WLAN-MAC-Adresse (für reine WLAN-Mobilgeräte).

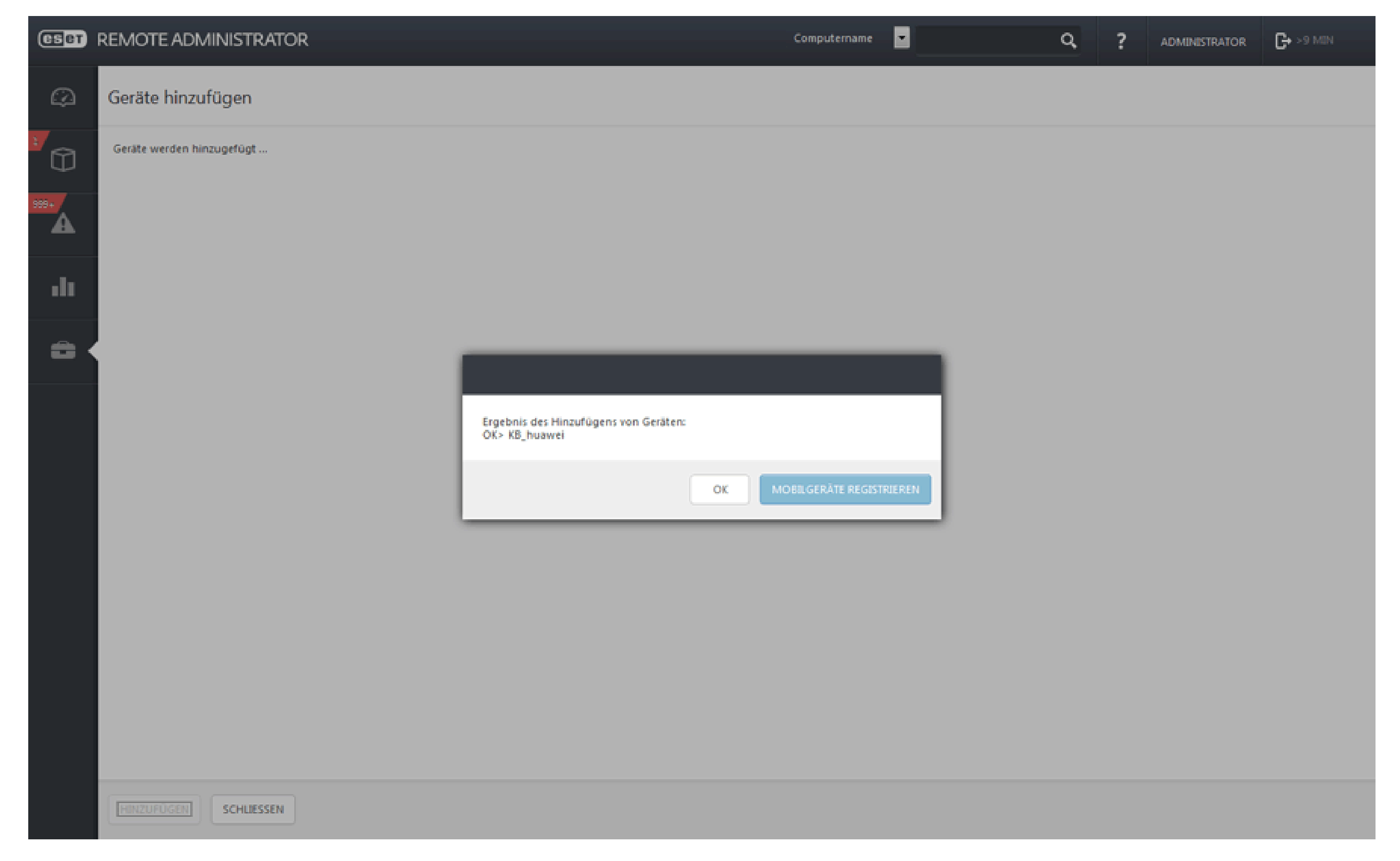


3. Mobile Geräte können auf zwei Arten registriert werden:

   a. Der Administrator erhält die MAC-Adresse des Geräts vorab und registriert das Gerät auf herkömmliche Weise in ERA

   b. Der Benutzer klickt auf einen (vom Administrator verschickten) Registrierungs-Link. In diesem Fall antwortet die App automatisch, dass das Gerät nicht in der Positivliste enthalten/nicht genehmigt ist, und zeigt die MAC-Adresse auf dem Bildschirm an. Der Benutzer wird aufgefordert, sich an den Administrator zu wenden und die Gerätenummer (MAC-Adresse) an ihn weiterzugeben.

4. Klicken Sie auf **Hinzufügen** und dann im Dialogfenster auf **Mobilgeräte registrieren**.



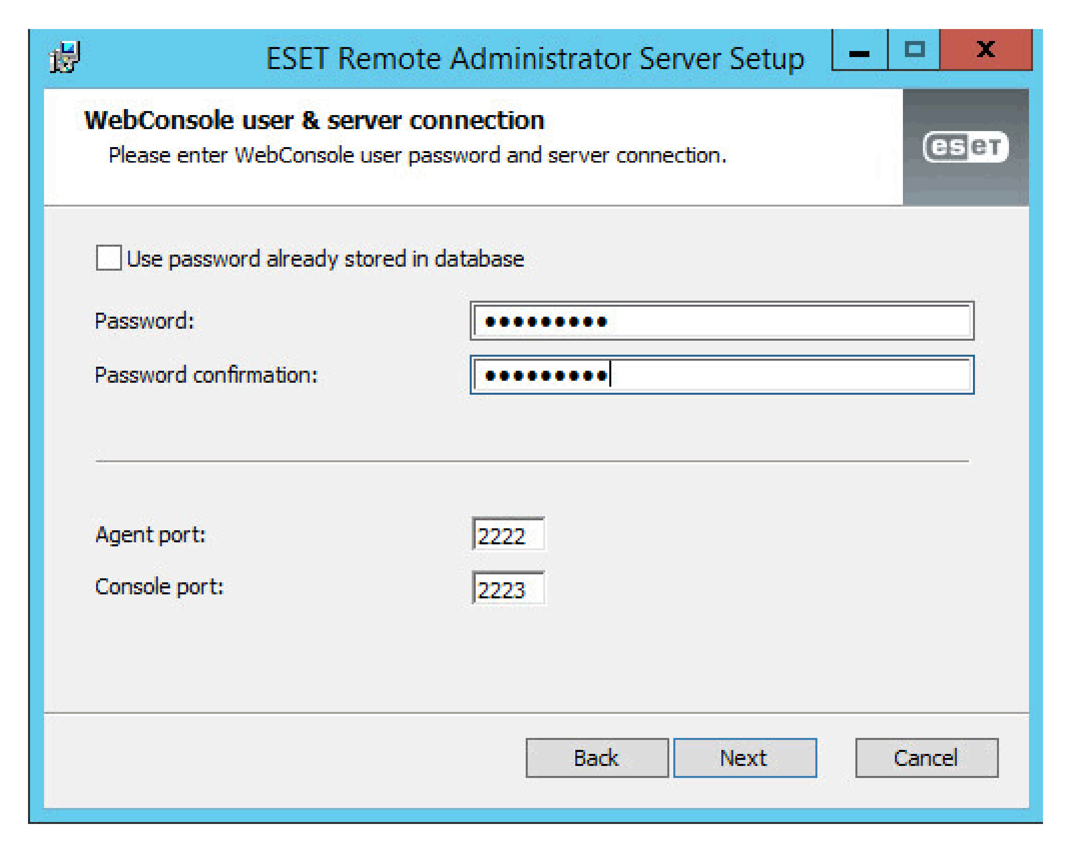
Der Assistent für den Task Mobilgeräteregistrierung führt Sie durch den Vorgang der Mobilgeräteregistrierung.

4.6 Bewährte Methoden

Passwort vergessen: Im Idealfall sollte das Administratorkonto nur zum Erstellen von Konten für einzelne Benutzer mit Administratorrechten verwendet werden. Nachdem Administratorkonten erstellt wurden, sollte das Administratorpasswort sicher aufbewahrt und das Administratorkonto nicht verwendet werden. Auf diese Weise kann das Administratorkonto dazu verwendet werden, bei Bedarf die Passwörter/Kontodetails der Benutzer mit Administratorrechten zurückzusetzen.

So können Sie das **Passwort eines eingebauten ERA-Administratorkontos ändern**:

- Öffnen Sie **Programme und Funktionen** (führen Sie appwiz.cpl aus), suchen Sie den ESET Remote Administrator-Server und klicken Sie ihn mit der rechten Maustaste an
- Wählen Sie den Eintrag **Ändern** im Kontextmenü aus
- Wählen Sie **Reparieren aus**
- Geben Sie die Details der Datenbankverbindung ein
- Wählen Sie **Vorhandene Datenbank verwenden** aus und führen Sie das Upgrade durch
- Deaktivieren Sie die Option **Benutzerpasswort ist bereits in der Datenbank gespeichert** und geben Sie ein neues Passwort ein.
- Sie können sich nun mit Ihrem neuen Passwort bei der ERA Web-Konsole anmelden



4.6.1 Benutzerverwaltung

Es wird dringend empfohlen, zusätzliche Konten mit eingeschränkten Zugriffsrechten zu erstellen, die den erforderlichen Berechtigungen entsprechen.

5. Die Arbeit mit ESET Remote Administrator

Alle Clients werden über die ERA **Web-Konsole** verwaltet. Sie können mit einem beliebigen Gerät mit kompatiblem Browser auf die Web-Konsole zugreifen. Die Web-Konsole ist in drei Hauptbereiche unterteilt:

1. Oben in der Web-Konsole befindet sich das **Schnellsuche**-Tool. Geben Sie einen **Clientnamen** oder eine **IPv4/ IPv6-Adresse** ein und klicken Sie dann auf das Lupensymbol der drücken Sie die **Eingabetaste**. Sie werden zum Bereich Gruppen geleitet, wo die übereinstimmenden Clients angezeigt wird.

2. Im Menü auf der linken Seite finden Sie die Hauptbereiche von ESET Remote Administrator sowie folgende Quick Links:

- Dashboard
- Computer
- Bedrohungen
- Berichte
- Admin

Quick Links

- Neuer Systembenutzer
- Neue Policy
- Neuer Clienttask
- Live-Installationsprogramme für Agenten

3. Die Schaltflächen unten auf der Seite hängen vom Bereich und der Funktion ab und werden ausführlich in den entsprechenden Kapiteln beschrieben.

HINWEIS: Eine Schaltfläche wird für alle neuen Elemente angezeigt: **Pflichteinstellungen**. Diese rote Schaltfläche wird angezeigt, wenn Pflichteinstellungen nicht konfiguriert wurden und die Erstellung nicht fortgesetzt werden kann. Dies wird außerdem durch ein rotes Ausrufezeichen neben dem entsprechenden Bereich angezeigt. Klicken Sie auf **Pflichteinstellungen**, um zum betreffenden Bereich mit den fehlenden Einstellungen zu navigieren.

Allgemeine Regeln

- Pflichteinstellungen (obligatorische Einstellungen) sind immer mit einem roten Ausrufezeichen gekennzeichnet. Klicken Sie unten auf der Seite auf **Pflichteinstellungen**, um (sofern zutreffend) die Pflichteinstellungen zu öffnen.
- Wenn Sie Hilfe mit der Verwendung von ESET Remote Administrator benötigen, klicken Sie oben rechts auf das **?**-Symbol oder blättern Sie links zum Seitenende und klicken Sie auf **Hilfe**, um die Hilfeseiten zu öffnen. Das entsprechende Hilfefenster für die aktuelle Seite wird angezeigt.
- Im Bereich **Admin** werden besondere Konfigurationseinstellungen vorgenommen. Weitere Informationen hierzu finden Sie im Kapitel Admin.

5.1 Dashboard

Das Dashboard ist die Standardseite, die bei der ersten Anmeldung des Benutzers bei der ERA Web-Konsole angezeigt wird. Es zeigt vordefinierte Berichte über das Netzwerk an. Über die Registerkarten in der oberen Menüleiste können Sie zwischen den Dashboards wechseln. Jedes Dashboard besteht aus mehreren Berichten. Sie können die Dashboards anpassen, indem Sie Berichte hinzufügen oder bearbeiten oder die Größe, Position und Anordnung der Berichte ändern. All diese Informationen bieten einen umfassenden Überblick über ESET Remote Administrator und die Komponenten (Clients, Gruppen, Tasks, Policies, Benutzer, Kompetenzen usw.). In ESET Remote Administrator gibt es vier vorkonfigurierte Dashboards:

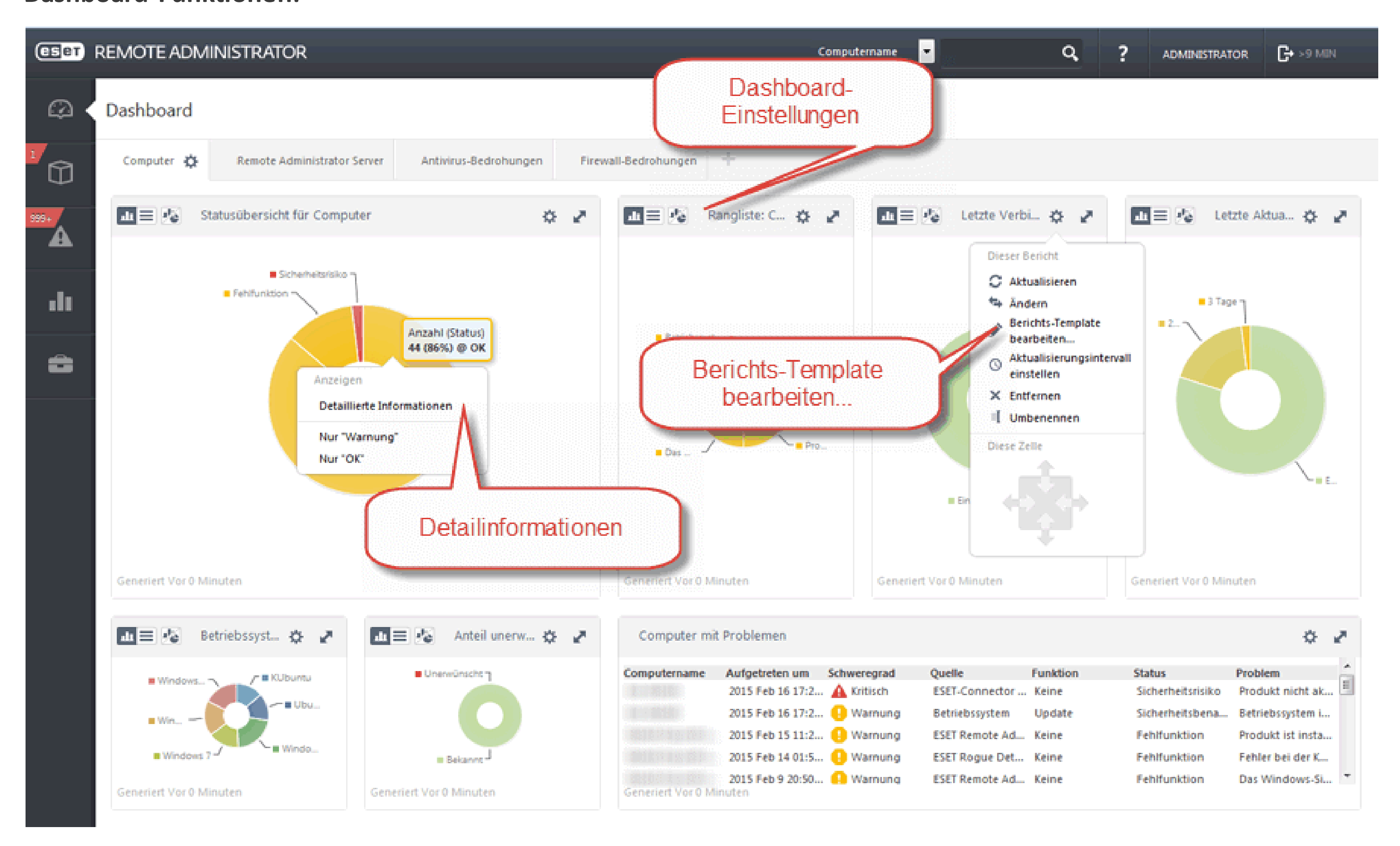
Computer
Dieses Dashboard enthält eine Übersicht der Clientcomputer: ihr Schutzstatus, Betriebssystem, Update-Status usw.

Remote Administrator Server
In diesem Dashboard finden Sie Informationen zum ESET Remote Administrator-Server: Serverlast, Clients mit Problemen, CPU-Auslastung, Datenbankverbindungen usw.

Antivirus-Bedrohungen
Hier werden Bericht des Virenschutzes der Client-Sicherheitsmodule angezeigt: aktive Bedrohungen, Bedrohungen in den letzten 7/30 Tagen usw.

Firewall-Bedrohungen
Firewall-Ereignisse der verbundenen Clients, nach Schweregrad, Zeitpunkt der Erfassung usw.

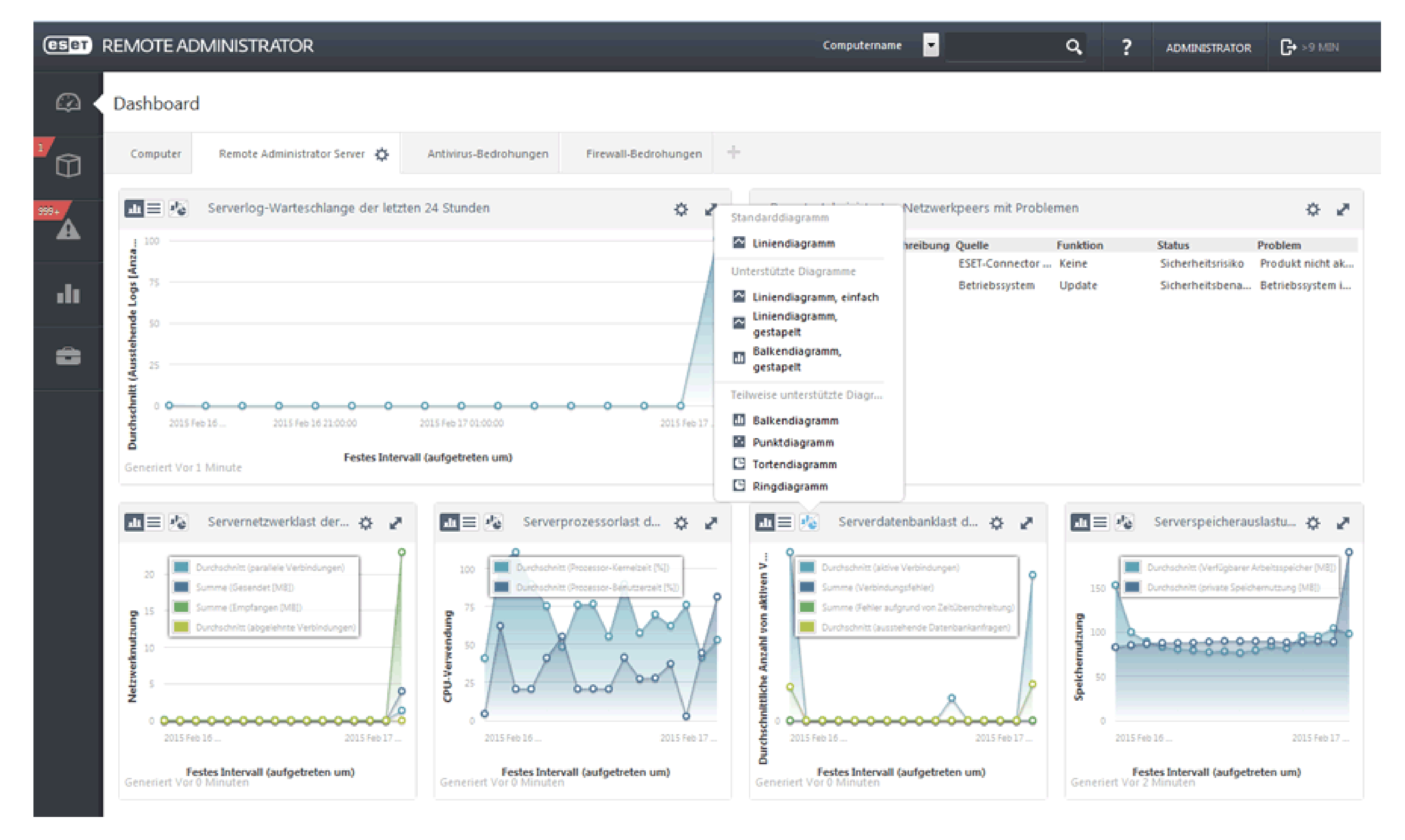
Dashboard-Funktionen:



5.1.1 Dashboard-Einstellungen

Dashboard-Einstellungen sind sowohl für vordefinierte als auch für neu erstellte Dashboards verfügbar und dienen der Verwaltung der Dashboards. Die verfügbaren Optionen werden nachstehend beschrieben:

- **Neues Dashboard hinzufügen** – Klicken Sie auf das Symbol + oben in der Kopfzeile des Dashboards. Geben Sie einen Namen für das neue Dashboard ein und klicken Sie zum Bestätigen auf **OK**. Ein neues Dashboard ohne Inhalte im Berichtfeld wird erstellt. Nach dem Einrichten des Dashboards können Sie Berichte zu ihm hinzufügen.
- **Dashboard duplizieren** – Wählen Sie das zu duplizierende Dashboard aus und klicken Sie neben dem Dashboardnamen auf das **Zahnradsymbol** ⚙. Wählen Sie **Duplizieren** in der Liste aus. Ein Duplikat des Dashboards wird erstellt.
- **Dashboard verschieben** – Klicken Sie auf den Namen eines Dashboards und ziehen Sie es an eine andere Stelle, um seine Position in Bezug auf die anderen Dashboards zu ändern.
- **Dashboardgröße (Anzahl der angezeigten Berichte) ändern** – Klicken Sie auf das **Zahnradsymbol** ⚙ > **Layout ändern**. Wählen Sie die Anzahl der im Dashboard anzuzeigenden Berichte aus (Ziehen) und klicken Sie darauf. Das Dashboardlayout wird geändert.
- **Dashboard umbenennen** – Klicken Sie auf das **Zahnradsymbol** ⚙ neben dem Dashboardnamen und klicken Sie auf **Umbenennen**. Geben Sie einen neuen Namen für das Dashboard ein und klicken Sie auf **OK**.
- **Dashboard entfernen** – Klicken Sie auf das **Zahnradsymbol** ⚙ neben dem Dashboardnamen, klicken Sie auf **Entfernen** und bestätigen Sie Ihre Auswahl.
- **Größe ändern** – Klicken Sie auf das **Doppelpfeilsymbol** rechts neben einem Bericht, um seine Größe zu ändern. Wichtigere Berichte sollten größer, weniger wichtige Berichte kleiner dargestellt werden. Sie können einen Bericht auch im Vollbildmodus anzeigen.



- **Diagrammtyp ändern**: Klicken Sie oben links in einem Diagramm auf das Symbol **Diagramm** und ändern Sie den Typ in **Tortendiagramm**, **Liniendiagramm** usw., um den Diagrammtyp zu ändern.
- Klicken Sie auf **Aktualisieren**, um die angezeigten Informationen zu aktualisieren.
- Klicken Sie auf **Ändern**, um einen anderen Bericht anzuzeigen.
- Klicken Sie auf Bericht-Template bearbeiten, um ein Template hinzuzufügen oder zu bearbeiten.
- Klicken Sie auf **Aktualisierungsintervall einstellen**, um festzulegen, wie häufig die Daten im Bericht aktualisiert werden sollen. Das standardmäßige Aktulisierungsintervall ist 120 Sekunden.
- **Umbenennen/Entfernen**: Über diese Schaltflächen können Sie einen Bericht umbenennen oder entfernen.

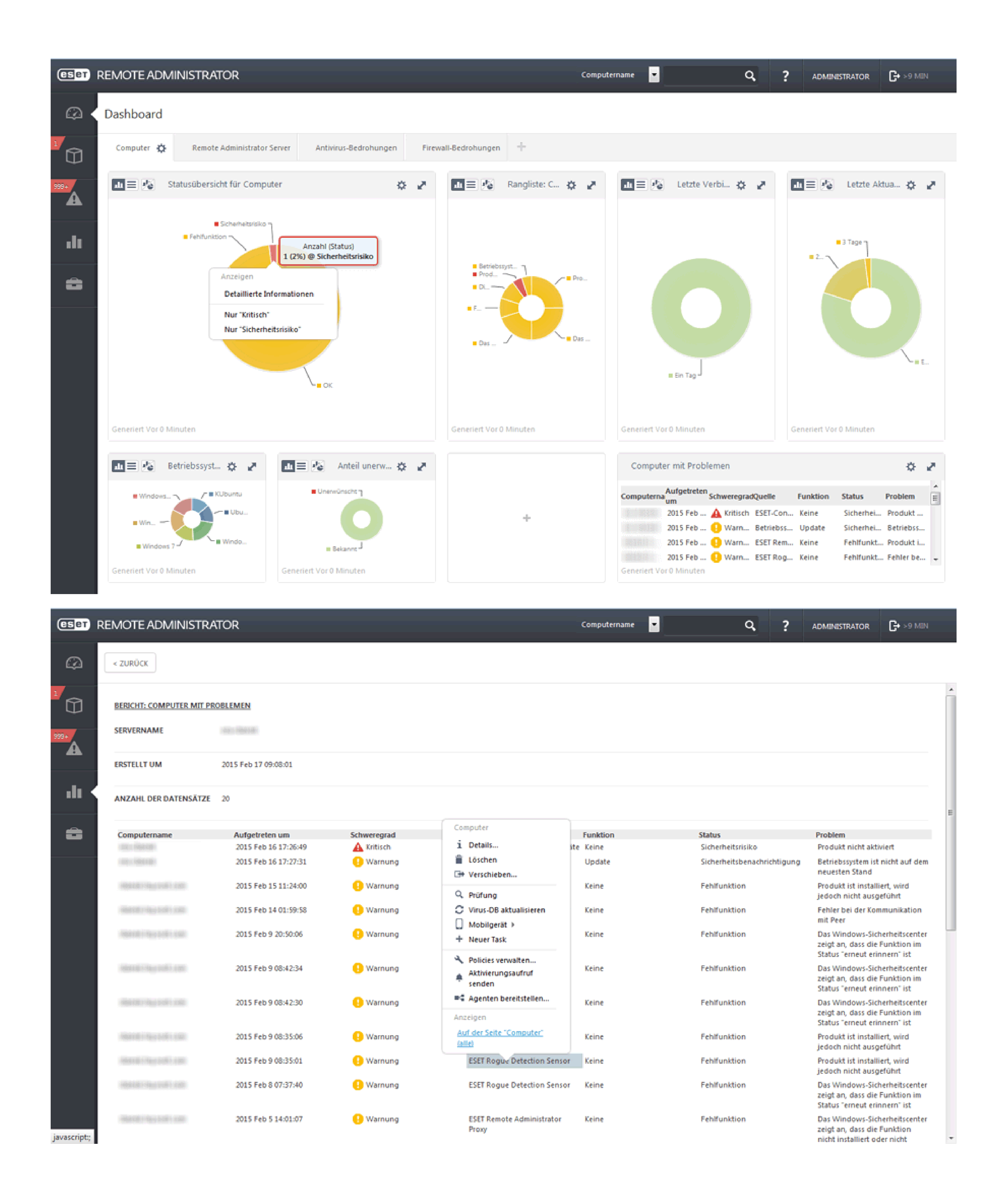
5.1.2 Detailinformationen

Mit dieser Dashboardfunktion können Sie die Daten genauer untersuchen. Hier können Sie interaktiv bestimmte Elemente aus der Übersicht auswählen und detaillierte Daten dazu anzeigen lassen. Sie können sich also von den Übersichtsinformationen ins Detail „herunterarbeiten“, um weitere Informationen zum Element anzuzeigen. Meistens stehen mehrere Detailebenen zur Verfügung.

Es gibt vier Detailtypen:

- **Detaillierte Informationen** anzeigen - Computername und -beschreibung, Name der statischen Gruppe usw. Zeigt die ursprünglichen (nicht zusammengefasste) Daten für die ausgewählte Zeile an.
- **Nur '*Wert*'** anzeigen: Information, schwerwiegend, Sicherheitsrisiko, Sicherheitsbenachrichtigung usw.
- **Spalte '*Wert*' erweitern** - Zeigt das Detail der zusammengefassten Informationen (in der Regel für eine Anzahl oder Summe) an. Wenn die Spalte beispielsweise nur eine Zahl enthält und Sie auf **Spalte 'Computer' erweitern** klicken, werden alle Details zu den Computern aufgeführt.
- **Auf der Seite "Computer" (alle)** - leitet Sie zur Seite „Computer“ weiter (zeigt ein Ergebnis mit 100 Elementen an).

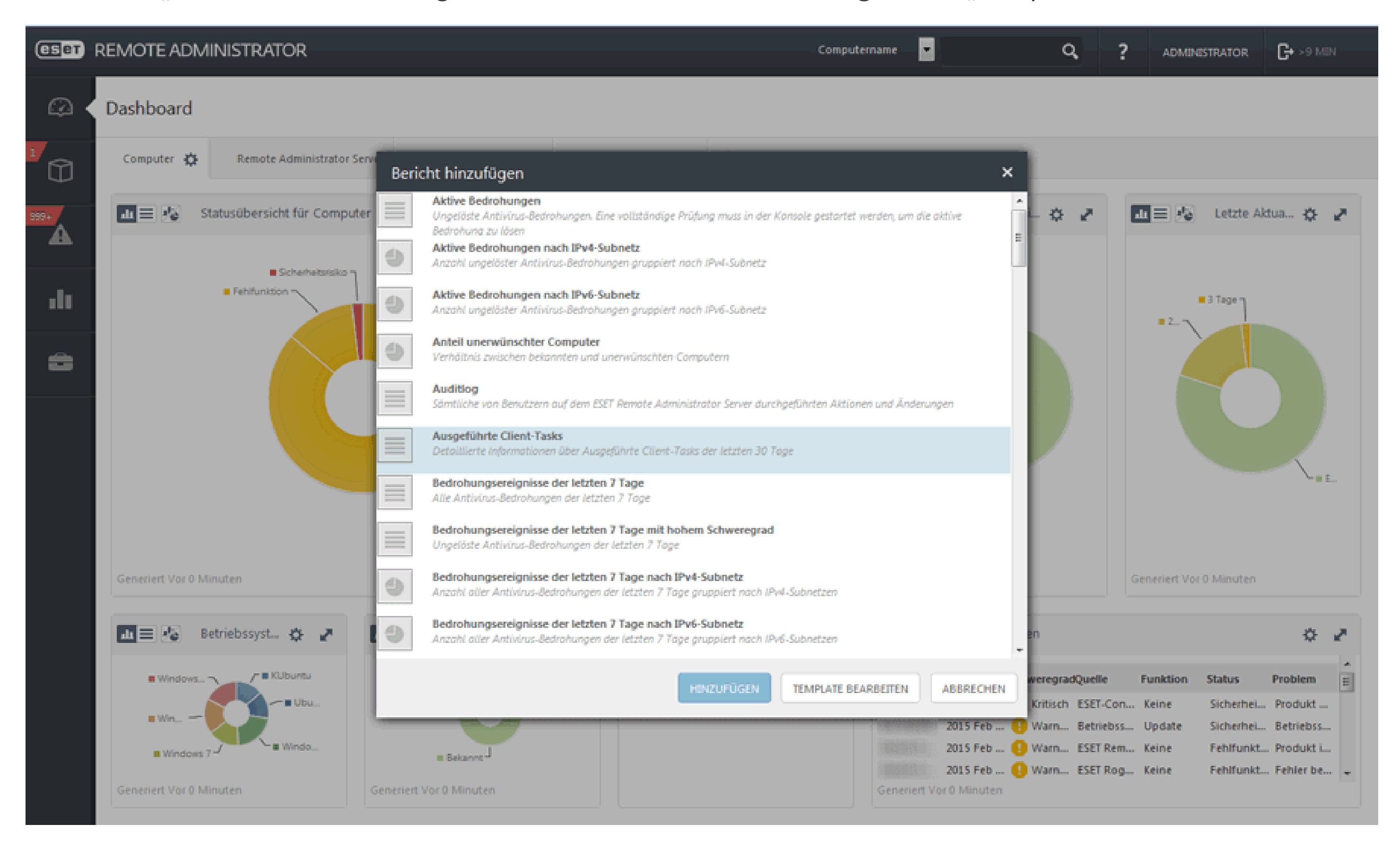
HINWEIS: Beim Anzeigen von Detailinformationen in anderen Berichten werden nur die ersten 1000 Elemente angezeigt.


REMOTE ADMINISTRATOR
Computername
ADMINISTRATOR
Dashboard
Computer
Remote Administrator Server
Antivirus-Bedrohungen
Firewall-Bedrohungen
Statusübersicht für Computer
Sicherheitsrisiko
Fehlfunktion
Anzahl (Status)
1 (2%) @ Sicherheitsrisiko
Anzeigen
Detaillierte Informationen
Nur "Kritisch"
Nur "Sicherheitsrisiko"
OK
Rangliste: C...
Letzte Verbi...
Ein Tag
Letzte Aktua...
3 Tage
Generiert Vor 0 Minuten
Betriebssyst...
KUbuntu
Windows 7
Anteil unerw...
Unerwünscht
Bekannt
Computer mit Problemen
Computername
Aufgetreten um
Schweregrad
Quelle
Funktion
Status
Problem
2015 Feb ...
Kritisch
ESET-Con...
Keine
Sicherhei...
Produkt ...
Warn...
Betriebss...
Update
ESET Rem...
Fehlfunkt...
Produkt i...
ESET Rog...
Fehler be...
< ZURÜCK
BERICHT: COMPUTER MIT PROBLEMEN
SERVERNAME
ERSTELLT UM
2015 Feb 17 09:08:01
ANZAHL DER DATENSÄTZE
20
Computer
Details...
Löschen
Verschieben...
Prüfung
Virus-DB aktualisieren
Mobilgerät
Neuer Task
Policies verwalten...
Aktivierungsaufruf senden
Agenten bereitstellen...
Anzeigen
Auf der Seite "Computer" (alle)
2015 Feb 16 17:26:49
Kritisch
Sicherheitsrisiko
Produkt nicht aktiviert
2015 Feb 16 17:27:31
Warnung
Sicherheitsbenachrichtigung
Betriebssystem ist nicht auf dem neuesten Stand
2015 Feb 15 11:24:00
Fehlfunktion
Produkt ist installiert, wird jedoch nicht ausgeführt
2015 Feb 14 01:59:58
Fehler bei der Kommunikation mit Peer
2015 Feb 9 20:50:06
Das Windows-Sicherheitscenter zeigt an, dass die Funktion im Status "erneut erinnern" ist
2015 Feb 9 08:42:34
2015 Feb 9 08:42:30
2015 Feb 9 08:35:06
2015 Feb 9 08:35:01
ESET Rogue Detection Sensor
2015 Feb 8 07:37:40
2015 Feb 5 14:01:07
ESET Remote Administrator Proxy
Das Windows-Sicherheitscenter zeigt an, dass die Funktion nicht installiert oder nicht
javascript:;

5.1.3 Bericht-Template bearbeiten

Dieser Abschnitt beschreibt das Bearbeiten vorhandener Bericht-Templates. Informationen zum Erstellen neuer Bericht-Templates finden Sie hier.

Klicken Sie auf das **leere Quadrat** im neuen Dashboard. Das Fenster zum Hinzufügen eines Berichts wird angezeigt. Wählen Sie „Installierte Anwendungen“ aus und klicken Sie auf **Hinzufügen** oder „Template bearbeiten“.

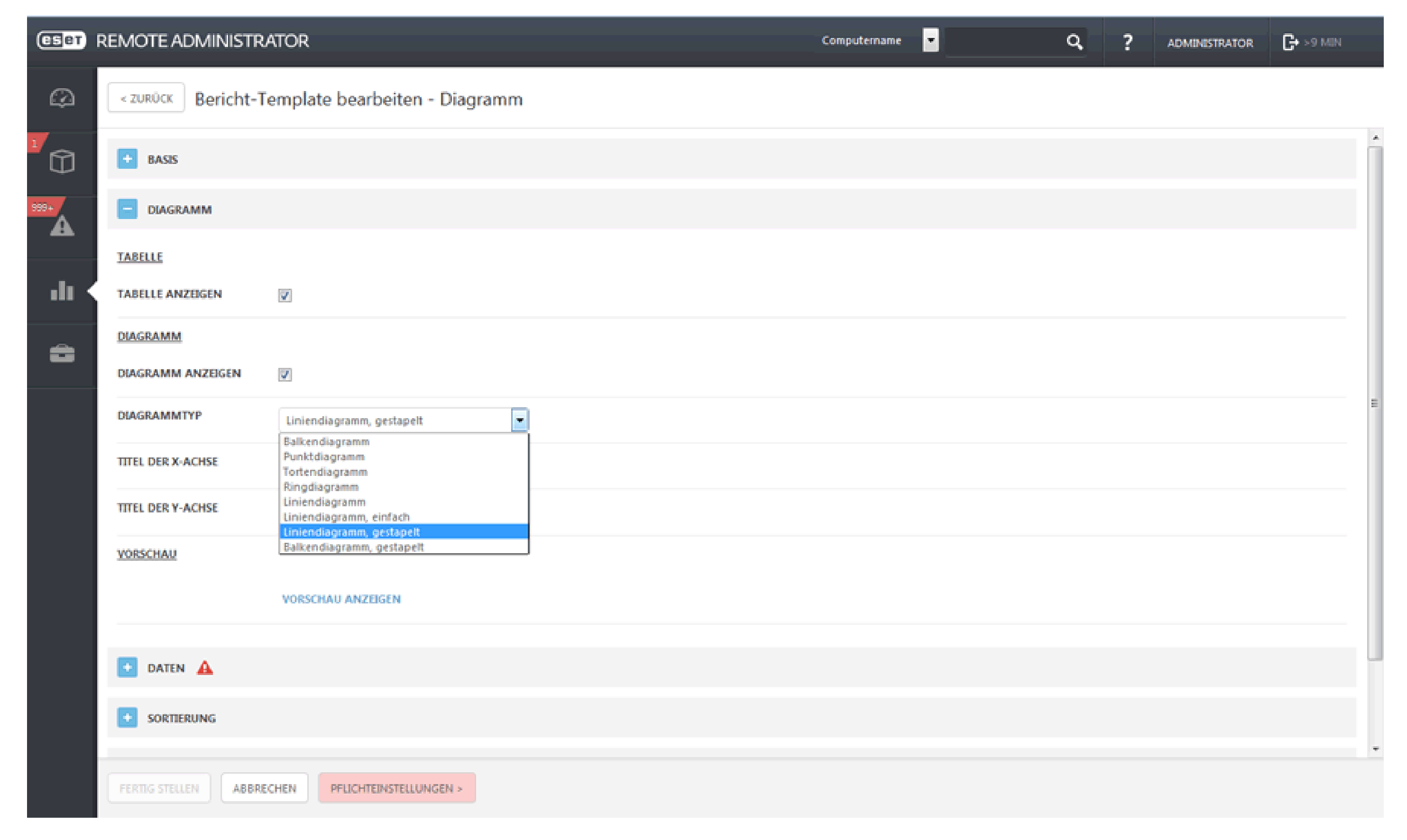


Basis

Bearbeiten Sie die grundlegenden Informationen zum Template im Bereich **Basis**. Hier können Sie den **Namen**, die **Beschreibung** und die **Kategorie** überprüfen oder ändern. Diese Informationen werden auf Grundlage des ausgewählten **Bericht**typs vordefiniert.

Diagramm

Wählen Sie im Abschnitt **Diagramm** den Typ **Bericht** aus. In diesem Beispiel lassen wird die Option **Tabelle anzeigen** leer und wählen die Option **Diagramm anzeigen** aus.

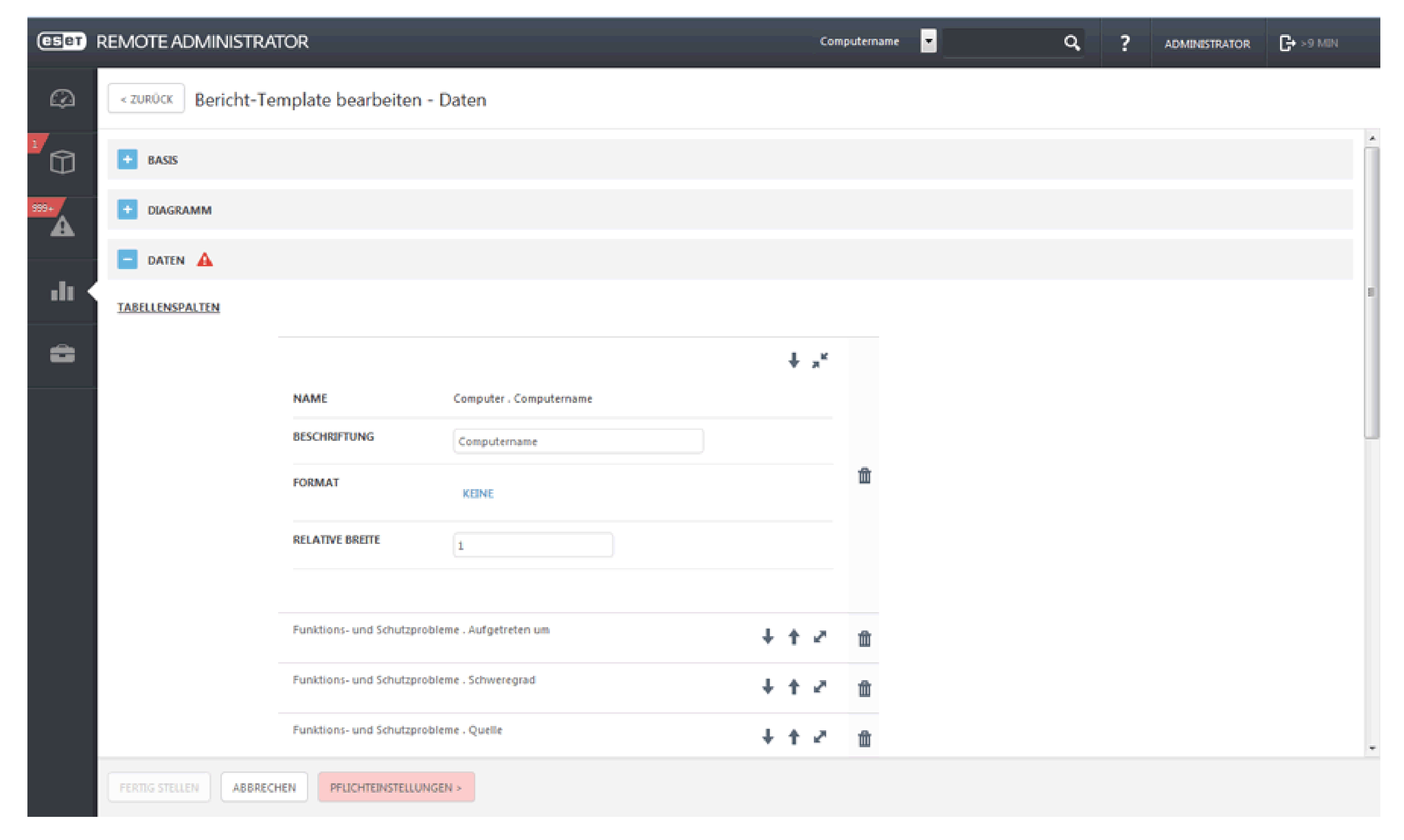


HINWEIS: Jeder ausgewählte Diagrammtyp wird im Abschnitt **Vorschau** angezeigt. So können Sie in Echtzeit sehen, wie der Bericht aussehen wird.

Bei der Auswahl eines **Diagramms** stehen mehrere Optionen zur Verfügung. Zur besseren Übersichtlichkeit wählen wir hier den Diagrammtyp **Liniendiagramm, gestapelt** aus. Dieser Diagrammtyp ist hilfreich, wenn Sie Daten mit unterschiedlichen Maßeinheiten analysieren möchten.

Optional können Sie für die **X**- und **Y**-Achse des Diagramms eine Beschriftung festlegen, um die Analyse des Diagramms zu erleichtern.

Daten



Geben Sie im Abschnitt **Daten** die Informationen ein, die an der **X**- und **Y**-Achse des Diagramms angezeigt werden sollen. Wenn Sie auf die entsprechenden Symbole klicken, wird ein Fenster mit Optionen angezeigt. Die für die **Y**-Achse verfügbaren Optionen hängen von den Informationen ab, die für die **X**-Achse ausgewählt wurden (und umgekehrt), weil das Diagramm ihre Beziehung zueinander darstellt und die Daten hierzu kompatibel sein müssen.

In unserem Beispiel wählen wir für die **X**-Achse **Computer** > **Computername** aus, um zu ermitteln, welche Computer Spam senden. Das **Format** wird auf **Wert** > **Absolut** festgelegt. Der Administrator legt die Farbe und Symbole fest.

Für die **Y**-Achse wählen wir **Installierte Software** > **Größe in MB**, um die absolute Menge Spam-Meldungen zu ermitteln. Das **Format** wird auf **Wert** > **Absolut** festgelegt. Der Administrator legt die Farbe und Symbole fest.

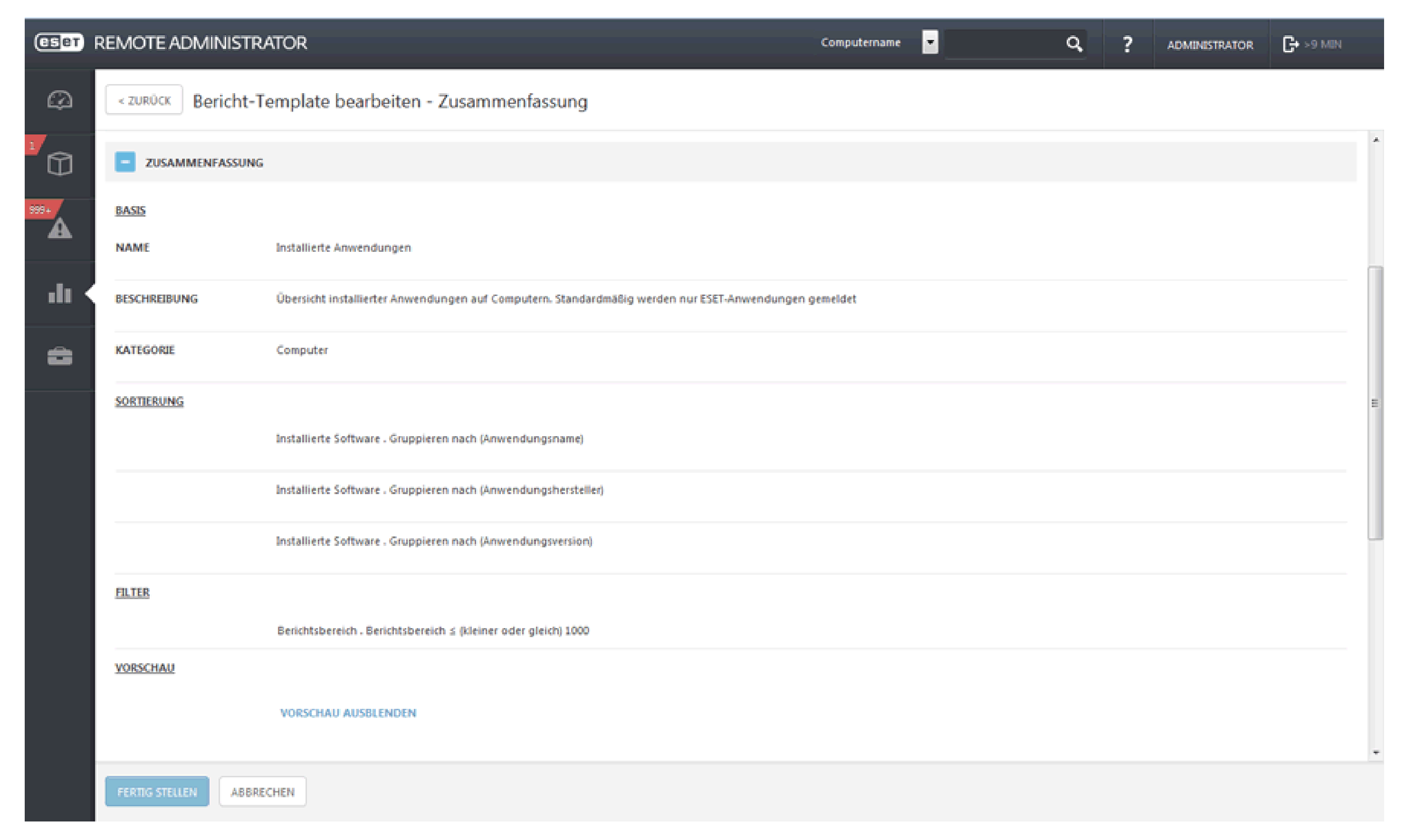
Sortierung

Über Sortierung hinzufügen können Sie eine Beziehung zwischen den ausgewählten Daten definieren. Wählen Sie die Ausgangsinformationen und dann die Sortiermethode **Aufsteigend** oder **Absteigend** aus. Die Daten können auch über beide Optionen sortiert werden (siehe oben).

Filter

Die hier angezeigten Optionen hängen von den zuvor konfigurierten Einstellungen ab (Informationen der X- und Y-Achse). Wählen Sie eine Option und eine mathematische Funktion aus, um festzulegen, wie die Daten gefiltert werden sollen. In diesem Beispiel wählen wir **Installierte Software** und **Anwendungsname** > **ist gleich** > **ESS** und **Installierte Software**. **Größe in MB** > **ist größer als** > **50**.

Zusammenfassung



Überprüfen Sie in der **Zusammenfassung** die ausgewählten Optionen und Informationen. Wenn Sie keine Änderungen vornehmen möchten, klicken Sie auf **Fertig stellen**, um ein neues **Bericht-Template** zu erstellen.

5.2 Computer

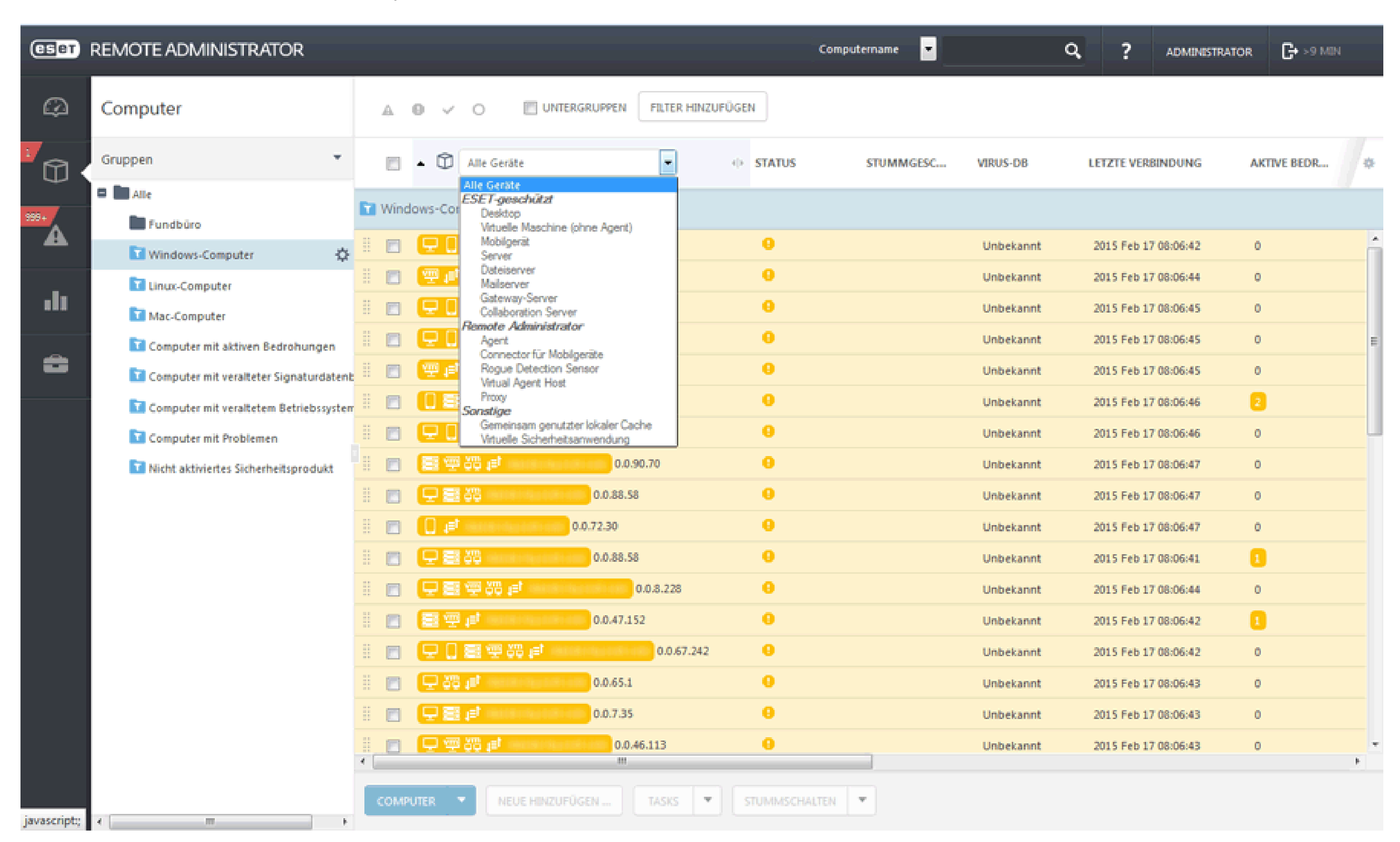
Alle Clientcomputer, die zu ESET Remote Administrator hinzugefügt wurden, werden hier in Gruppen sortiert angezeigt. Wenn Sie links in der Liste auf eine Gruppe klicken, werden die Mitglieder (Clients) der Gruppe rechts angezeigt. Sie können die Clients mit den Filtern oben an der Seite filtern. Klicken Sie auf **Filter hinzufügen**, um die verfügbaren Filterkriterien anzuzeigen. Außerdem stehen für den Schnellzugriff einige vordefinierte Filter zur Verfügung:

- Vier Symbole zum Filtern nach Schweregrad (rot – **Fehler**, gelb – **Warnungens**, grün – **Hinweise** und grau – **Nicht verwaltete** Computer). Das Symbol für den Schweregrad entspricht dem aktuellen Status des ESET-Produkts auf dem Clientcomputer. Sie können diese Symbole je nach Bedarf ein- und ausschalten und so kombinieren. Um beispielsweise nur Computer mit Warnungen anzuzeigen, lassen Sie nur das gelbe Symbol aktiviert und deaktivieren Sie die restlichen Symbole. Um Warnungen und Fehler anzuzeigen, aktivieren Sie nur die beiden entsprechenden Symbole.
- Kontrollkästchen **Untergruppen** – Untergruppen der ausgewählten Gruppe anzeigen.
- **Nicht verwaltete** Computer (Clients im Netzwerk ohne installierten ERA-Agent bzw. ohne installiertes ESET-Sicherheitsprodukt) werden üblicherweise in der Gruppe **Fundbüro** angezeigt.

Über das Dropdown-Menü unter den Filtern können Sie die Liste der angezeigten Clients (Computer) eingrenzen. Folgende Kategorien sind verfügbar:

- **Alle Geräte**: Wählen Sie dies im Dropdownmenü aus, um erneut alle Clientcomputer ohne Eingrenzung (ohne Filterung) anzuzeigen. Zum Eingrenzen der Ansicht können Sie die oben genannten Filteroptionen beliebig kombinieren.
- **Durch ESET geschützt** (durch ein ESET-Produkt geschützt)
- **Remote Administrator** (einzelne ERA-Komponenten wie Agent, RD Sensor, Proxy usw.)
- **Sonstige** (freigegebener lokaler Cache, virtuelle Appliance). Nachdem Sie Ihre Auswahl getroffen haben, werden nur die übereinstimmenden Clients angezeigt.

HINWEIS: Falls Sie einen bestimmten Computer nicht in der Liste finden, der bekannterweise in der ERA-Infrastruktur enthalten ist, überprüfen Sie, ob alle Filter deaktiviert sind.



Mit dem Kontextmenü (Zahnradsymbol ⚙) können Sie statische oder dynamische Gruppen erstellen, Neue Tasks erstellen oder weitere Aktionen auswählen.

Aktionen der Schaltfläche **Computer**:

+ Neu ...
Fügen Sie manuell Geräte hinzu, die nicht automatisch gefunden oder hinzugefügt werden.

ℹ Details ...
- **Basis** (Name, übergeordnete Gruppe, Gerät, Betriebssysteminformationen usw.)
- **Konfiguration** (Konfiguration, angewendete Policies usw.)
- **Ausgeführte Tasks** (Aufgetreten, Taskname, Tasktyp, Status, usw.)
- **Installierte Anwendungen -** (Name, Hersteller, Version, Deinstallations-Unterstützung durch den Agenten usw.)
- **Warnungen** (Problem, Status usw.)
- **Bedrohungen** (Alle Bedrohungsarten, Stummgeschaltet, Ursache, usw.)
- **Quarantäne** (Bedrohungsname, Bedrohungstyp, Objektname, Hash usw.)

Löschen
Hiermit wird der Client aus der Liste entfernt. Solange er jedoch im Netzwerk enthalten ist, wird er in der Gruppe „Fundbüro“ angezeigt.

Verschieben ...
Sie können einen Client in eine andere Gruppe verschieben. Wenn Sie diese Option auswählen, wird eine Liste der verfügbaren Gruppen angezeigt.

Policies verwalten ...
Eine Policy kann auch direkt einem Client (oder mehreren Clients) zugewiesen werden, nicht nur einer Gruppe. Wählen Sie diese Option aus, um die Policy den ausgewählten Clients zuzuweisen.

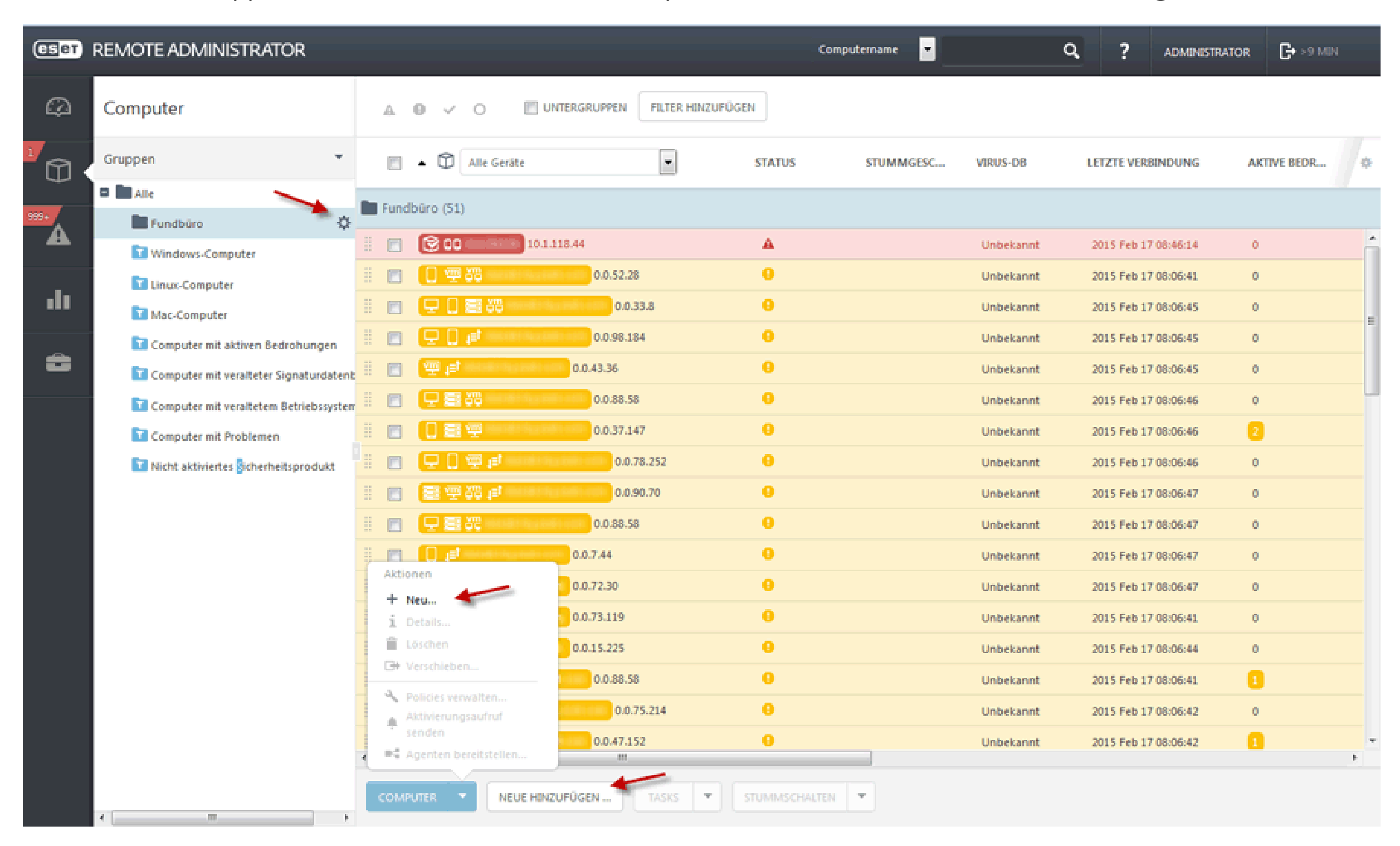
Aktivierungsaufruf senden
Der ERA-Server initiiert eine sofortige Kommunikation mit dem ERA-Agenten auf dem Clientcomputer. Dies ist nützlich, wenn Sie nicht auf das planmäßige Intervall warten möchten, in dem der ERA-Agent eine Verbindung zum ERA-Server herstellt. Dies ist z. B. hilfreich, wenn Sie einen Clienttask sofort auf einem oder mehreren Clients ausführen oder eine Policy umgehend anwenden möchten.

HINWEIS: Wenn Sie eine vorgenommene Änderung übernehmen möchten, warten Sie ca. eine Minute, bevor Sie den Aktivierungsaufruf senden.

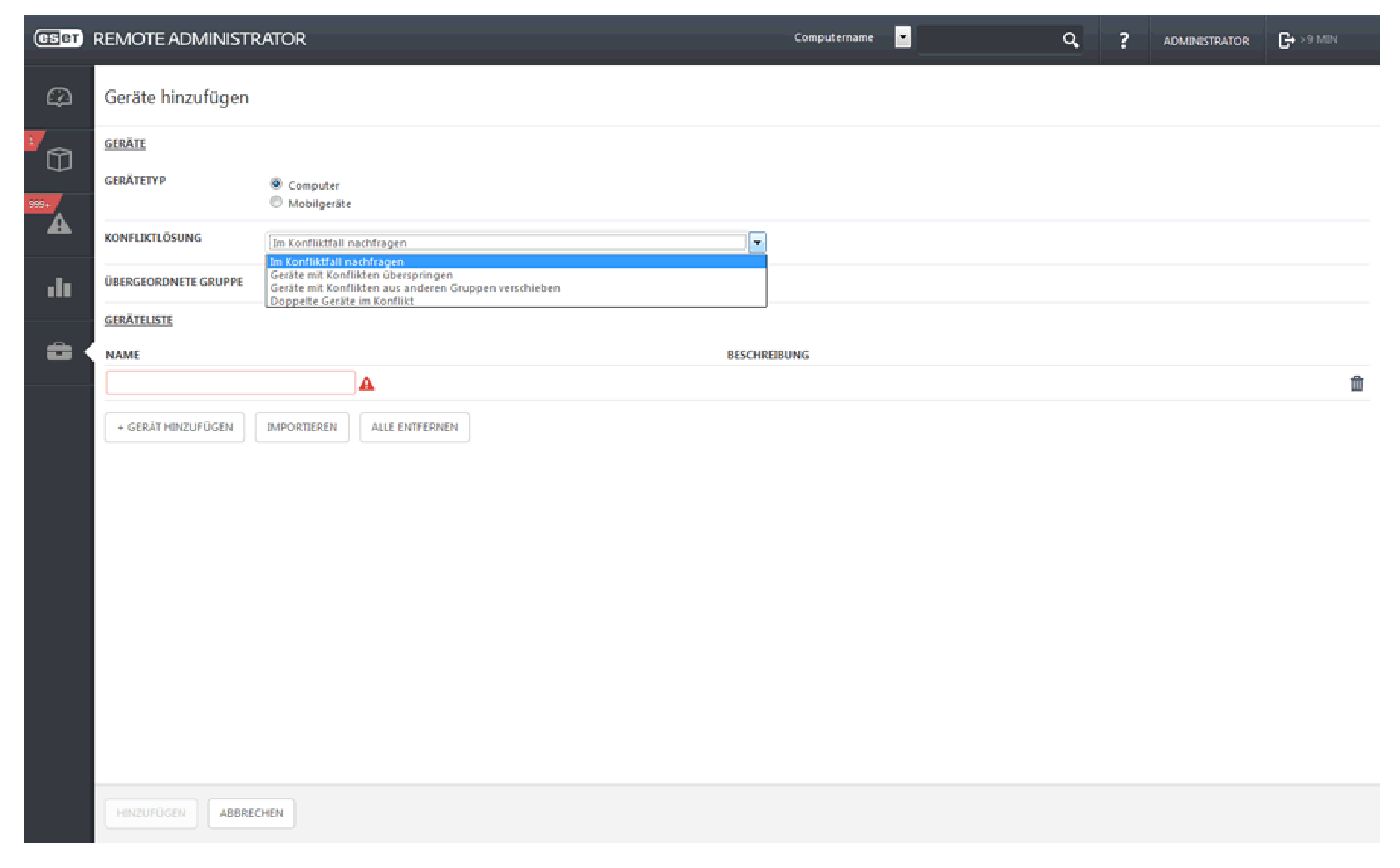
Agent bereitstellen ...
Mit dieser Option können Sie einen neuen Servertask erstellen.

5.2.1 Hinzufügen von Computern

Die **Registerkarte** Computer bietet drei Möglichkeiten zum Hinzufügen neuer Computer. Wählen Sie beispielsweise eine statische Gruppe aus, klicken Sie auf das Zahnradsymbol und wählen Sie + **Neue hinzufügen** aus.



Geben Sie den Namen des hinzuzufügenden Computers in das Feld **Name** ein. Klicken Sie auf + Gerät hinzufügen, um zusätzliche Computer hinzuzufügen, oder klicken Sie auf Importieren, um eine Datei mit einer Liste der hinzuzufügenden Computer zu importieren. Wahlweise können Sie eine **Beschreibung** für die Computer eingeben.



Im Dropdown-Menü „Konfliktlösung“ können Sie eine Aktion für den Fall auswählen, dass der Computer bereits in ERA vorhanden ist:

Im Konfliktfall nachfragen: Wenn ein Konflikt erkannt wird, fordert das Programm Sie zur Auswahl einer Aktion auf (siehe nachstehende Optionen).
Computer mit Konflikten überspringen: Bereits vorhandene Computer werden nicht hinzugefügt.
Computer mit Konflikten aus anderen Gruppen verschieben: Computer mit Konflikten werden aus der ursprünglichen Gruppe in die Gruppe **Alle** verschoben.
Computer mit Konflikten duplizieren: Neue Computer werden hinzugefügt, jedoch mit einem anderen Namen.

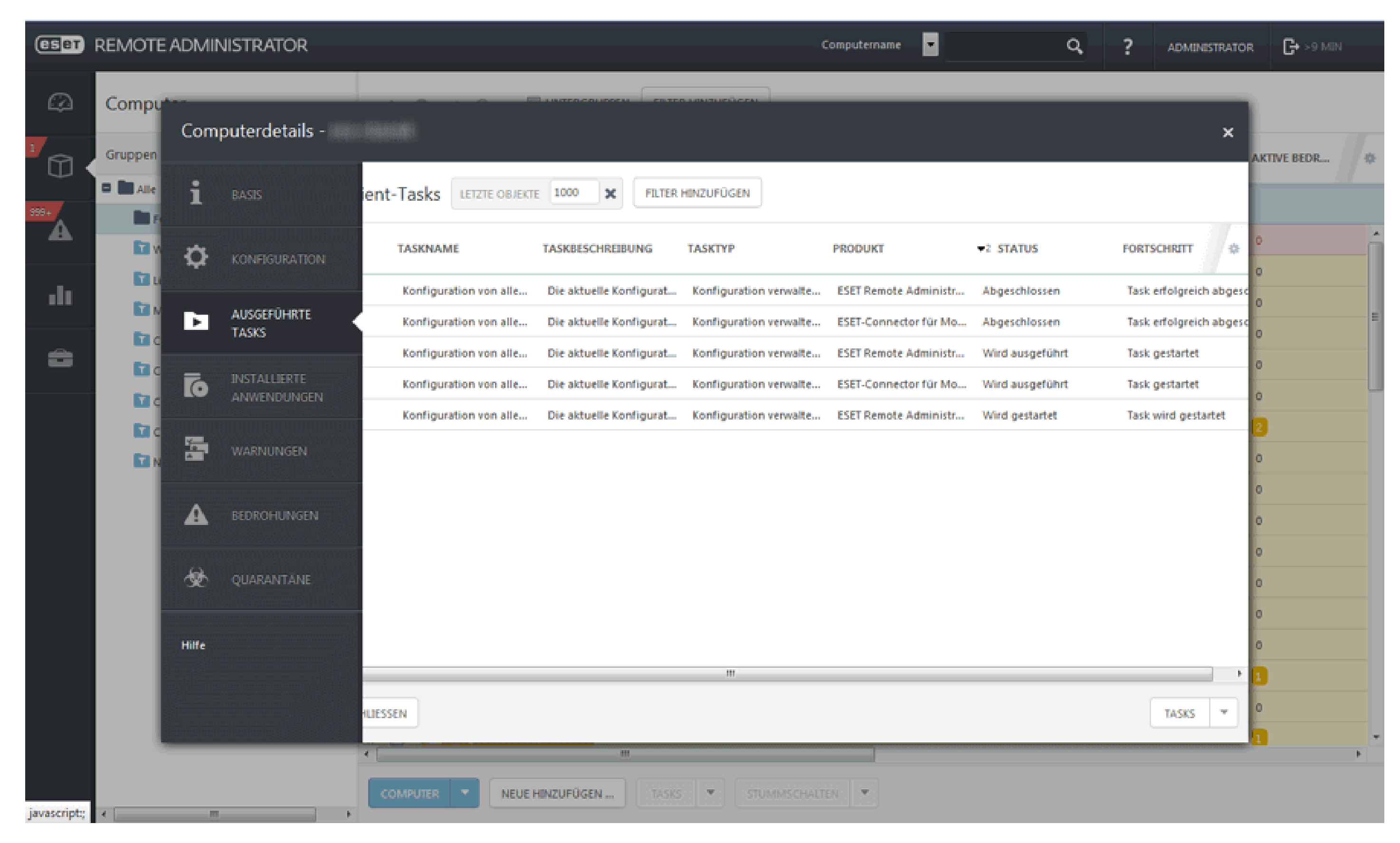
Klicken Sie auf **Hinzufügen**. Wenn Sie eine Gruppe auswählen, werden rechts in der Liste die zur Gruppe gehörenden Computer angezeigt.

HINWEIS: Das Hinzufügen mehrerer Computer kann einige Zeit in Anspruch nehmen, Reverse-DNS-Lookup kann durchgeführt werden.

Weitere Informationen zum Hinzufügen von Mobilgeräten finden Sie im Kapitel Mobilgeräteregistrierung.

5.2.2 Computerdetails

Wählen Sie einen Computer in einer statischen oder dynamischen Gruppe aus und klicken Sie auf **Details**, um weitere Informationen zum Computer anzuzeigen.



Das Menü „Computerdetails“ enthält folgende Einstellungen:

- **Basis** - Hier können Sie den Namen, die Beschreibung und die übergeordnete Gruppe des Computers ändern.
- **Konfiguration** - zeigt die gesamte Konfiguration, die Verbindung und die angewendeten Policies für den Computer an.
- **Ausgeführte Tasks -** aufgetreten, Taskname, Tasktyp, Status
- **Installierte Anwendungen -** Name, Version, Größe, Deinstallations-Unterstützung durch den Agenten
- **Warnungen** - Problem, Status usw.
- **Bedrohungen -** alle Bedrohungsarten, stummgeschaltet, Ursache usw.
- **Quarantäne -** Bedrohungsname, Typ, Objektname, Hash usw.

Tasks Aktionsschaltflächen

Nachdem Sie einen oder mehrere Computer ausgewählt und auf „Tasks“ geklickt haben, werden folgende Optionen verfügbar:

Scan
Mit dieser Option wird der Task On-Demand-Scan auf dem Client ausgeführt, der die Bedrohung gemeldet hat.

Update der Signaturdatenbank
Mit dieser Option wird der Task Update der Signaturdatenbank ausgeführt (löst manuell ein Update aus).

Mobilgerät

- **Registrieren ...** - Mit dieser Option können Sie einen neuen Clienttask erstellen.
- **Suchen** – Zum Anfordern der GPS-Koordinaten des Mobilgeräts.
- **Sperren** – Das Gerät wird gesperrt, wenn eine verdächtige Aktivität erkannt oder das Gerät als „vermisst" gekennzeichnet wird.
- **Entsperren** – Das Gerät wird entsperrt.
- **Alarm** – Löst remote einen lauten Alarm aus. Der Alarm wird auch ausgelöst, wenn das Gerät stumm geschaltet ist.
- **Daten löschen** – Alle auf dem Gerät gespeicherten Daten werden dauerhaft gelöscht.

+ Neuer Task ...

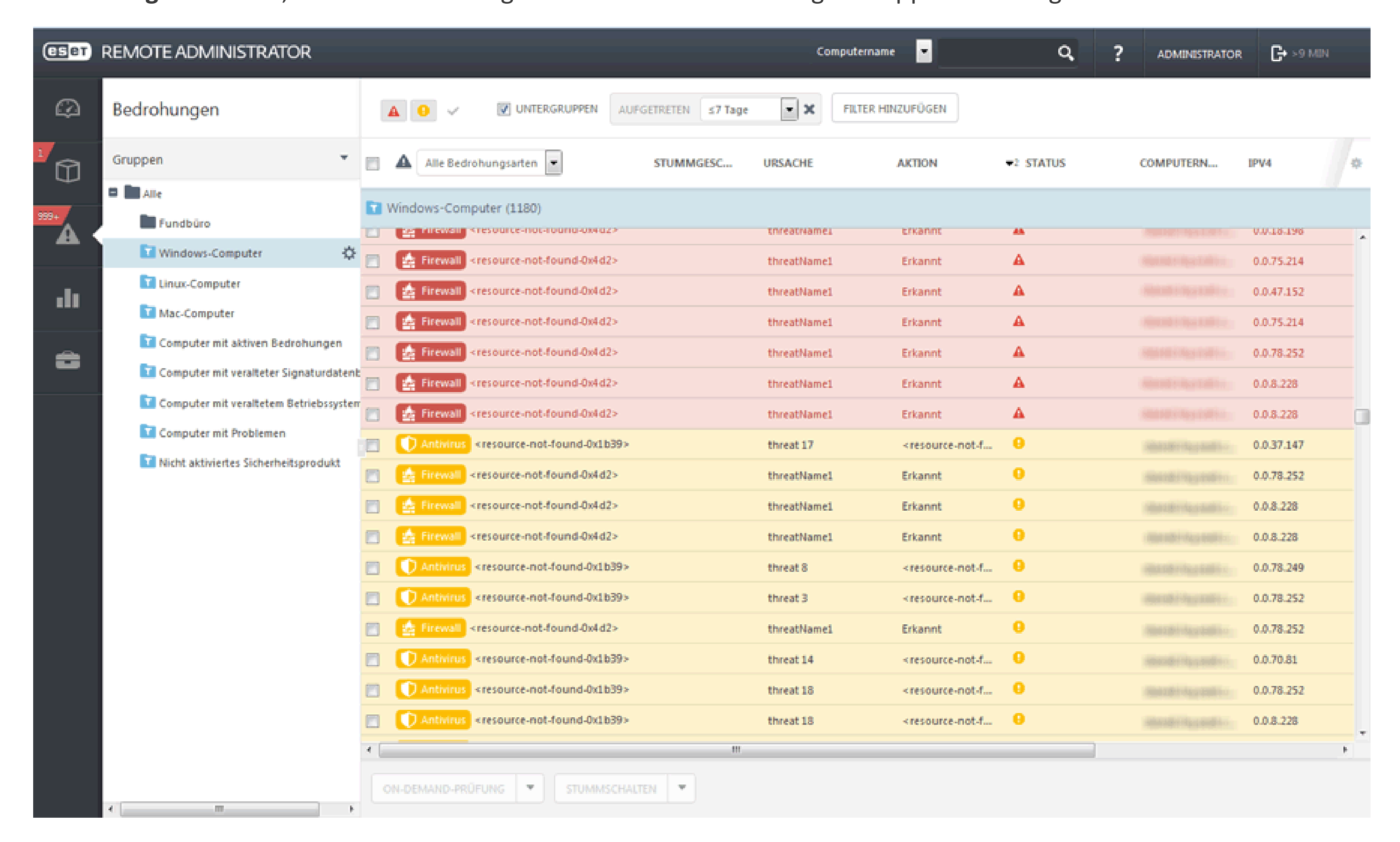
Wählen Sie einen Task aus und konfigurieren Sie (optional) die Drosselung für den Task. Der Task wird gemäß den Taskeinstellungen in die Warteschlange gesetzt.
Diese Option löst sofort einen vorhandenen Task aus, den Sie aus einer Liste der verfügbaren Tasks auswählen. Für diesen Task ist der Trigger nicht verfügbar, weil er sofort ausgeführt wird.

Stummschalten

Wenn Sie einen Computer auswählen und auf **Stummschalten** klicken, sendet der Agent des Client keine Informationen mehr an den ERA-Server, sondern sammelt diese nur. Neben dem Computernamen wird in der Spalte „Stummgeschaltet" das Stummschaltungssymbol angezeigt.
Wenn die Stummschaltung durch Klicken auf **Stummschalten** > **Stummschaltung aufheben** deaktiviert wird, sendet der Computer wieder Meldungen und die Kommunikation zwischen dem ERA-Server und dem Client wird wiederhergestellt.

5.3 Bedrohungen

Im Abschnitt **Bedrohungen** finden Sie eine Übersicht aller Bedrohungen, die auf den Computern in Ihrem Netzwerk gefunden wurden. Links wird die Struktur der Gruppen angezeigt. Hier können Sie die Gruppen durchsuchen und Bedrohungen auf Mitgliedern einer bestimmten Gruppe anzeigen. Wählen Sie die Gruppe **Alle** und den Filter **Alle Bedrohungsarten** aus, um alle Bedrohungen auf den Clients beliebiger Gruppen anzuzeigen.



Bedrohungen filtern

Sie können die Bedrohungen mithilfe des Filters über der Liste filtern. Standardmäßig werden alle Bedrohungsarten der letzten 7 Tage angezeigt. Um mehrere Filterkriterien zu verwenden, klicken Sie auf **Filter hinzufügen** und wählen Sie ein Element aus der Liste aus. Sie können die Ergebnisse nach **Name** (Name der Bedrohung), **Ursache** (Ursache der Bedrohung) oder **IPv4/IPv6** (Adresse des Client, der diese **Bedrohung** gemeldet hat) filtern.

Standardmäßig werden alle Bedrohungsarten angezeigt. Sie können sie jedoch nach **Viren-Schutz** und **Firewall** filtern, um nur bestimmte Elemente anzuzeigen.

On-Demand-Scan

Mit dieser Option wird der Task On-Demand-Scan auf dem Client ausgeführt, der die Bedrohung gemeldet hat.

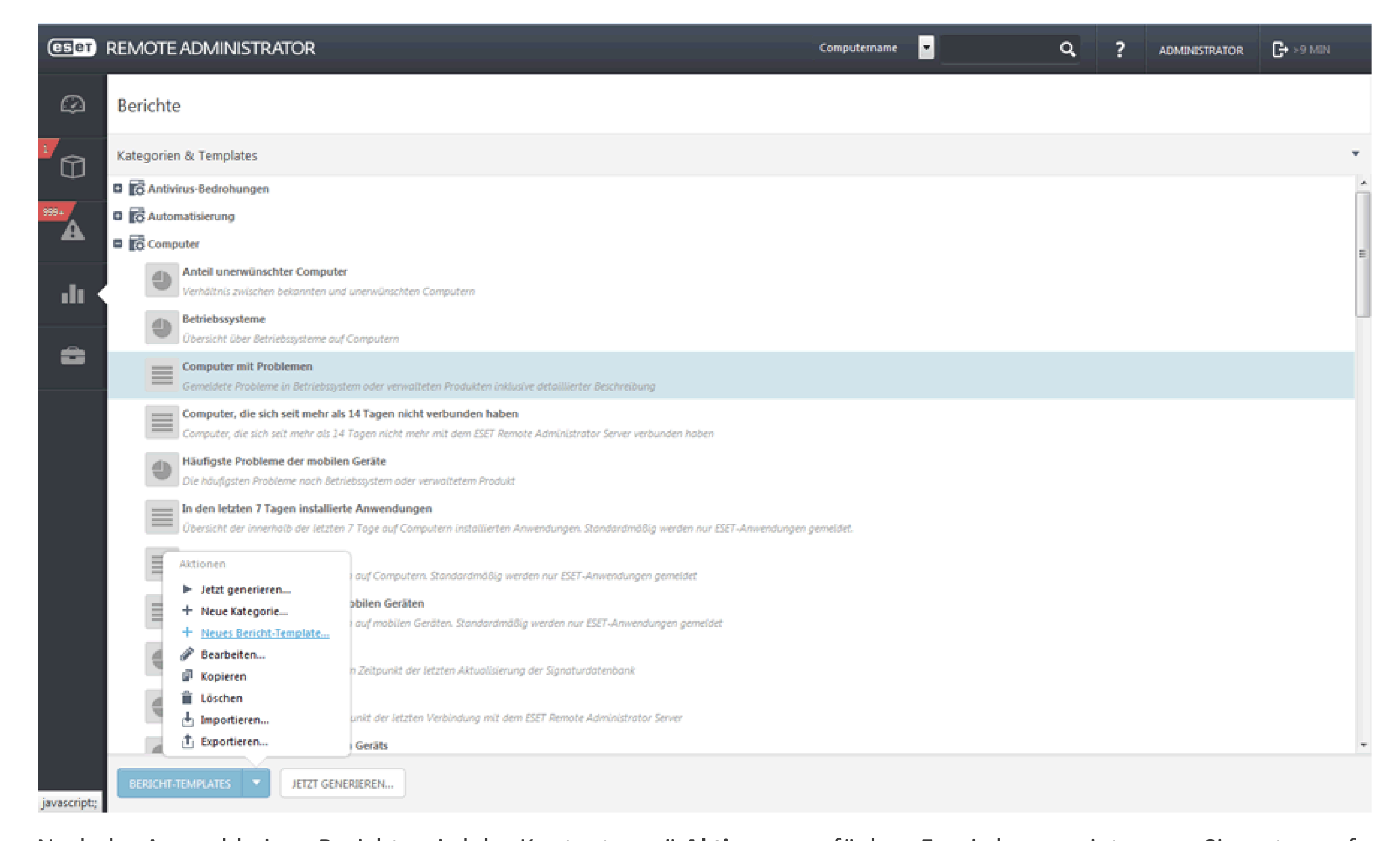
Stummschalten

Mit dieser Option wird die Bedrohung (nicht der Client) stummgeschaltet. Der Bericht wird nicht mehr als aktiv angezeigt. Sie können auch den Client, der die Bedrohung gemeldet hat, stummschalten (wählen Sie hierzu aus dem Kontextmenü der Bedrohung **Stummschalten** aus).

5.4 Berichte

Mit Berichten können Sie die Daten aus der Datenbank bequem filtern und auf sie zugreifen. Zur besseren Übersichtlichkeit sind die Berichte in Kategorien unterteilt. Jede Kategorie enthält auch eine kurze Beschreibung des Berichts. Klicken Sie unten auf der Seite auf **Jetzt generieren**, um einen Bericht auf Basis eines ausgewählten Templates zu erstellen und den Bericht anzuzeigen.

Sie können vordefinierte Bericht-Templates aus der Liste der **Kategorien und Templates** verwenden oder ein neues Bericht-Template mit benutzerdefinierten Einstellungen erstellen. Klicken Sie auf Neues Bericht-Template erstellen, um die Einstellungen für jeden Bericht im Detail anzuzeigen und benutzerdefinierte Einstellungen für einen neuen Bericht festzulegen.



Nach der Auswahl eines Berichts wird das Kontextmenü **Aktionen** verfügbar. Es wird angezeigt, wenn Sie unten auf der Seite auf **Bericht-Templates** klicken. Folgende Optionen stehen zur Verfügung:

Jetzt generieren ... - Wählen Sie aus der Liste einen Bericht aus und navigieren Sie zu **Bericht-Templates** > **Jetzt generieren ...** bzw. klicken Sie einfach auf **Jetzt generieren ...**. Der Bericht wird erstellt und Sie können die Ausgabedaten überprüfen.

+ **Neue Kategorie ...** - Geben Sie einen **Namen** und eine **Beschreibung** ein, um eine neue Kategorie für Bericht-Templates zu erstellen.

+ **Neues Bericht-Template ...** - Erstellen Sie ein neues benutzerdefiniertes Bericht-Template.

Bearbeiten ... - Bearbeiten Sie ein vorhandenes Bericht-Template. Es gelten die gleichen Einstellungen und Optionen wie beim Erstellen eines neuen Bericht-Templates (siehe oben).

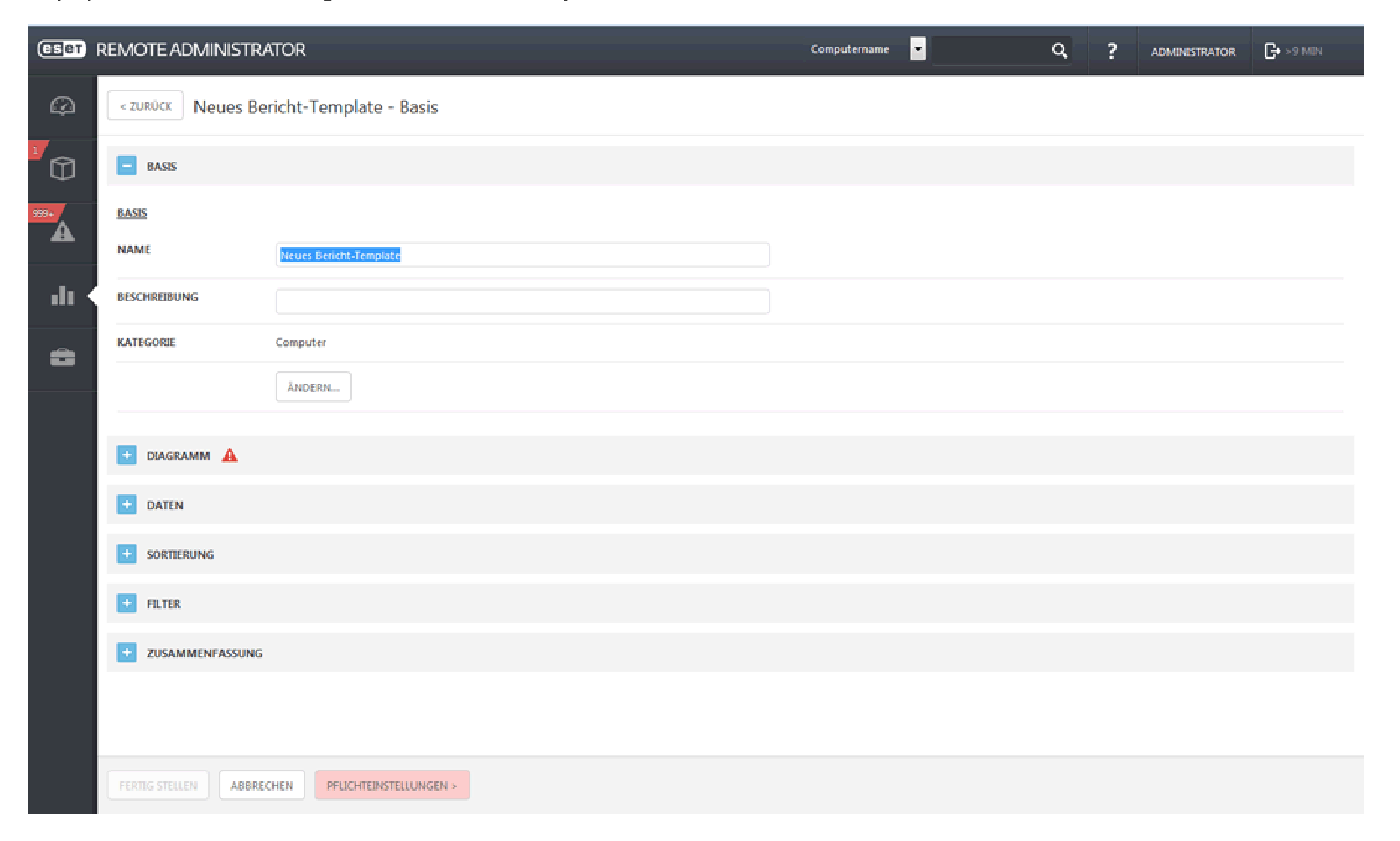
Kopieren - Verwenden Sie die Kopierfunktion nur, wenn Sie nur geringfügige Änderungen an einem bestehenden Bericht-Template vornehmen möchten. **Kopieren** Sie ein vorhandenes Bericht-Template und **Bearbeiten** Sie dann die Einstellungen, um ein neues Template zu erstellen.

Löschen - Entfernt das ausgewählte Bericht-Template vollständig.

Importieren/ Exportieren - Wählen Sie aus der Liste einen Bericht aus und navigieren Sie zu **Bericht-Templates** > **Exportieren...**. Der Bericht (mit den im Bericht definierten Daten) wird generiert und in einer *TXT*-Datei gespeichert.

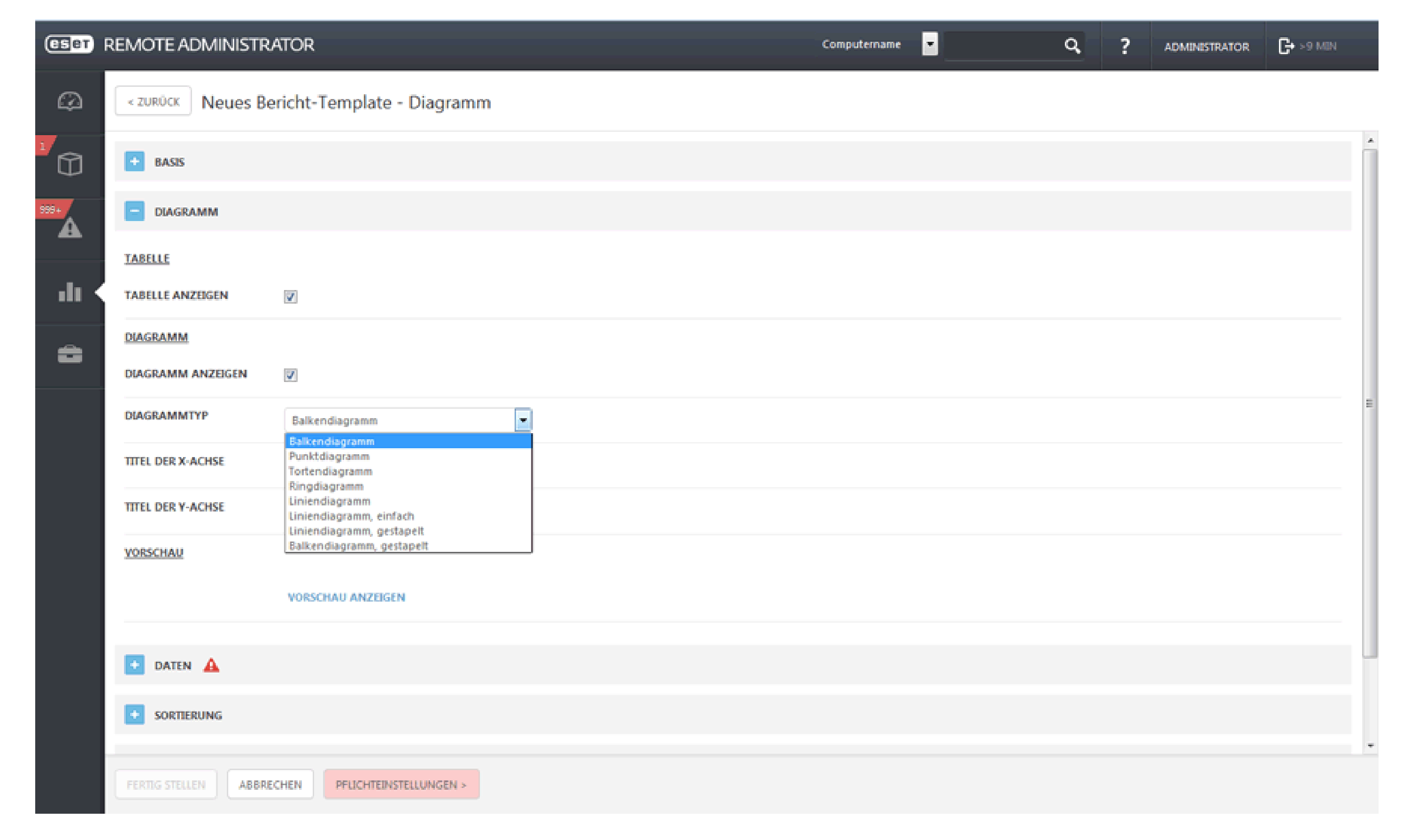
5.4.1 Erstellen eines neuen Bericht-Templates

Öffnen Sie **Berichte** und klicken Sie links unter **Kategorien & Templates** auf **Bericht-Templates**. Wählen Sie im Popup-Fenster den Eintrag **Neues Bericht-Template ...** aus.



Basis

Bearbeiten Sie die grundlegenden Informationen zum Template. Geben Sie einen **Namen**, eine **Beschreibung** und eine **Kategorie** ein. Sie können entweder eine vordefinierte Kategorie verwenden oder eine neue erstellen (verwenden Sie hierzu die im vorigen Kapitel beschriebene Option „Kategorie“).



Diagramm

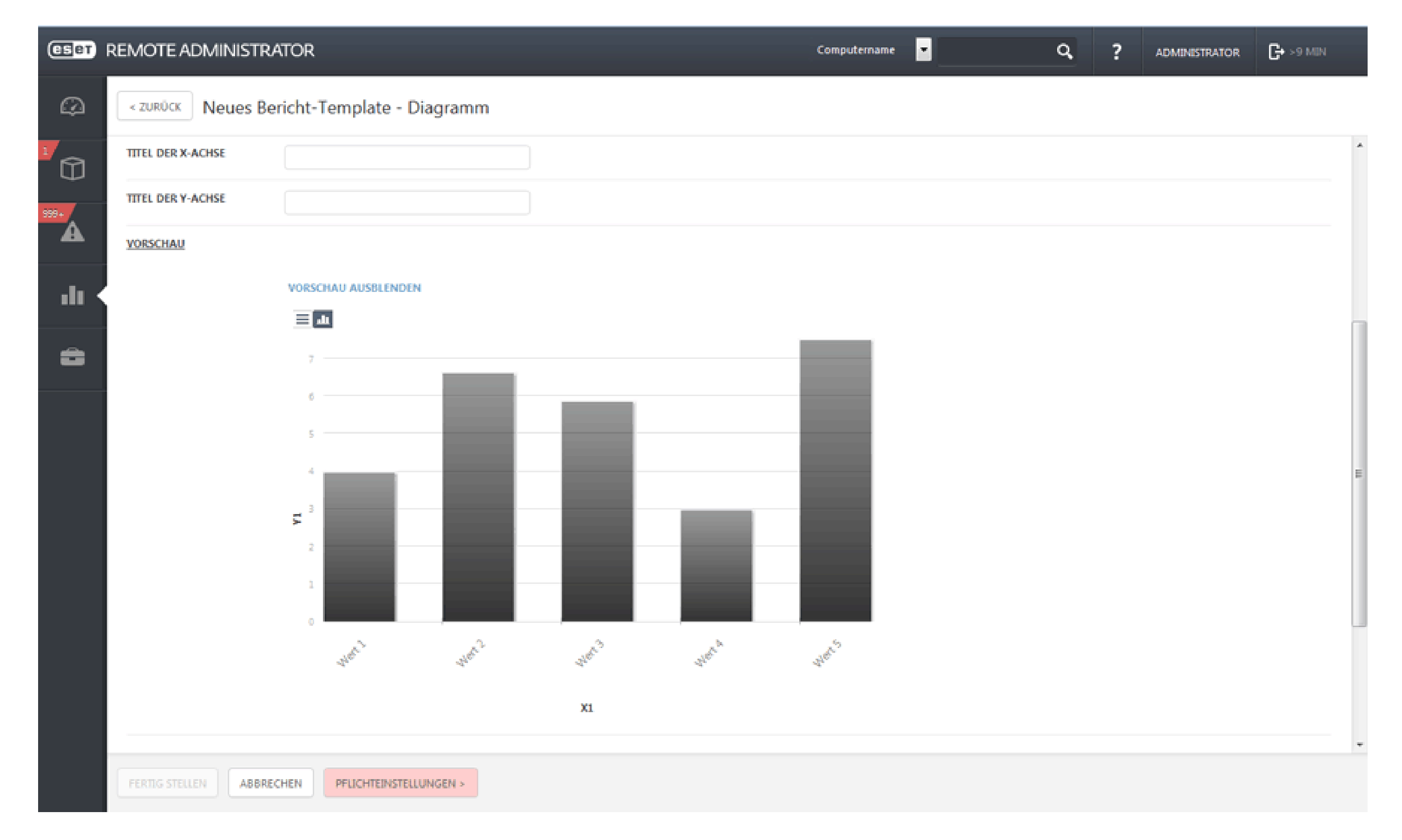
Wählen Sie im Abschnitt **Diagramm** den Typ **Bericht** aus. Wählen Sie entweder eine **Tabelle** aus, um die Informationen in Zeilen und Spalten anzuordnen, oder ein **Diagramm**, in dem die Daten an X- und Y-Achsen angezeigt werden.

HINWEIS: Der ausgewählte Diagrammtyp wird im Abschnitt **Vorschau** angezeigt. So können Sie in Echtzeit sehen, wie der Bericht aussehen wird.

Bei der Auswahl eines **Diagramms** stehen mehrere Optionen zur Verfügung:

- **Balkendiagramm** – Ein Diagramm mit rechteckigen Balken, deren Größe proportional zum dargestellten Wert ist.
- **Punktdiagramm** – Die quantitativen Werte werden mit Punkten dargestellt (ähnelt einem Balkendiagramm).
- **Tortendiagramm** – Ein Tortendiagramm ist ein kreisförmiges Diagramm, dessen einzelne Teile proportional zur Größe der dargestellten Werte sind.
- **Ringdiagramm** – Ähnelt dem Tortendiagramm, kann jedoch mehrere Datentypen enthalten.
- **Liniendiagramm** – Zeigt die Informationen als Reihe von Datenpunkten an, die durch gerade Linien verbunden sind.
- **Liniendiagramm, einfach** – Zeigt die Informationen als auf den Werten basierende Linie ohne Datenpunkte an.
- **Liniendiagramm, gestapelt** – Dieser Diagrammtyp ist hilfreich, wenn Sie Daten mit unterschiedlichen Maßeinheiten analysieren möchten.
- **Balkendiagramm, gestapelt** – Ähnelt dem einfachen Balkendiagramm, die Balken enthalten jedoch Werte verschiedener Maßeinheiten, die übereinander gestapelt sind.

Optional können Sie für die **X**- und **Y**-Achse des Diagramms eine Beschriftung eingeben, um die Analyse des Diagramms zu erleichtern.



Daten

Im Abschnitt **Daten** können Sie die anzuzeigenden Informationen auswählen:

a. **Tabellenspalten**: Die Informationen werden automatisch auf Grundlage des ausgewählten Berichttyps in die Tabelle eingefügt. Sie können die Angaben unter **Name**, **Beschriftung** und **Format** anpassen (siehe unten).

b. **Diagrammachsen**: Wählen Sie die Daten für die **X**- und **Y**-Achse aus. Wenn Sie auf die entsprechenden Symbole klicken, wird ein Fenster mit Optionen angezeigt. Die für die **Y**-Achse verfügbaren Optionen hängen von den Informationen ab, die für die **X**-Achse ausgewählt wurden (und umgekehrt), weil das Diagramm ihre Beziehung zueinander darstellt und die Daten hierzu kompatibel sein müssen. Wählen Sie die gewünschten Informationen aus und klicken Sie auf **OK**.

Sie können das **Format** zur Anzeige der Daten ändern:
- **Datenleiste** (nur für Balkendiagramme) / **Wert** / **Farbe** / **Symbole**

Sortierung

Über **Sortierung hinzufügen** können Sie eine Beziehung zwischen den ausgewählten Daten definieren. Wählen Sie die Ausgangsinformationen (Sortierwert) und die Sortiermethode **Aufsteigend** oder **Absteigend** aus. Diese Angaben definieren die Ausgabe im Diagramm.

Filter

Legen Sie als nächstes die Filtermethode fest. Wählen Sie aus der Liste das Filterkriterium und einen Wert aus. Der Filter legt fest, welche Informationen im Diagramm angezeigt werden.

Zusammenfassung

Überprüfen Sie in der **Zusammenfassung** die ausgewählten Optionen und Informationen. Wenn Sie keine Änderungen vornehmen möchten, klicken Sie auf **Fertig stellen**, um ein neues Bericht-Template zu erstellen.

Für jeden Bericht im Dashboard stehen eigene Optionen zur Anpassung zur Verfügung. Klicken Sie oben rechts auf das Zahnradsymbol, um die Optionen anzuzeigen. Hier können Sie die angezeigten Optionen **Aktualisieren**, den Bericht in einen anderen Bericht **Ändern**, das Bericht-Template **Bearbeiten** (siehe oben beschriebene Optionen), ein neues Intervall für das **Aktualisieren** der Daten im Bericht festlegen oder den Bericht **Umbenennen**/**Entfernen**. Über die Pfeil im Symbol unten können Sie die Größe des Berichts anpassen. Gestalten Sie beispielsweise wichtige Berichter größer, weniger wichtige Berichte kleiner. Klicken Sie auf **Vollbildmodus ein/aus**, um den Bericht im Vollbildmodus anzuzeigen.

5.4.2 Bericht generieren

Ein Template kann auf zwei verschiedene Weisen erstellt oder bearbeitet werden:

1. Navigieren Sie zu **Admin** > **Tasks** > **Server-Tasks**. Wählen Sie **Neu ...** aus, um einen neuen Berichtgenerierungstask zu erstellen.
2. Wählen Sie zum Erzeugen des Berichts ein Bericht-Template aus. Sie können ein vordefiniertes Bericht-Template verwenden und bearbeiten oder ein neues Bericht-Template erstellen.

- Sie können den Bericht entweder per E-Mail senden (in einem hier festgelegten Dateiformat) oder in einer Datei speichern. Durch Klicken auf eine der Optionen werden die entsprechendem Einstellungen angezeigt.
- Konfigurieren Sie die Einstellungen (wie für den Task Bericht erzeugen beschrieben) und klicken Sie auf **Fertig stellen**.
- Der Task ist nun erstellt und wird in der Liste der **Tasktypen** angezeigt. Wählen Sie den Task aus und klicken Sie unten auf der Seite auf **Jetzt ausführen**. Der Task wird sofort ausgeführt.

5.4.3 Planen eines Berichts

1. Navigieren Sie zu **Admin** > **Tasks** > **Server-Tasks**. Wählen Sie **Neu** aus, um einen neuen Task vom Typ **Bericht generieren** zu erstellen.
2. Wählen Sie zum Erzeugen des Berichts ein Bericht-Template aus. Sie können ein vordefiniertes Bericht-Template verwenden und bearbeiten oder ein neues Bericht-Template erstellen.

- Sie können den Bericht entweder per E-Mail senden (in einem hier festgelegten Dateiformat) oder in einer Datei speichern. Durch Klicken auf eine der Optionen werden die entsprechendem Einstellungen angezeigt.
- Konfigurieren Sie die Einstellungen (wie für den Task Bericht erzeugen beschrieben). Erstellen wir dieses Mal einen **Servertrigger** für den Task.
- Navigieren Sie unter **Trigger** zu **Einstellungen**. Wählen Sie **Geplanter Trigger** aus und geben Sie an, wann der Task ausgeführt werden soll.
- Klicken Sie auf **Fertig stellen**. Der Task wird erstellt und zum hier definierten Zeitpunkt (einmalig oder wiederholt) ausgeführt.

5.4.4 Veraltete Anwendungen

Rufen Sie den Bericht mit dem Namen **Veraltete Anwendungen** auf, um anzuzeigen, welche ERA-Komponenten veraltet sind.

Dies können Sie auf zwei Arten tun:

1. Fügen Sie ein Neues Dashboard hinzu. Klicken Sie auf eine der Kacheln, um ein Popup-Fenster mit der Liste der **Bericht-Templates** anzuzeigen. Wählen Sie den Bericht **Veraltete Anwendungen** aus der Liste aus und klicken Sie auf **Hinzufügen**.
2. Navigieren Sie im Bereich **Berichte** zur Kategorie **Computer**, wählen Sie die Vorlage **Veraltete Anwendungen** aus der Liste aus und klicken Sie unten auf die Schaltfläche **Jetzt generieren...**. Der Bericht wird erstellt und Sie können die Ausgabedaten überprüfen.

Mit dem Client-Task Upgrade von Administrator-Komponenten können Sie die Komponenten aktualisieren.

6. Verwaltung von ESET Remote Administrator

Im Abschnitt Verwaltung von ESET Remote Administrator wird die Verwaltung und Konfiguration von ESET Remote Administrator erläutert. Lesen Sie weiter im Kapitel Admin.

6.1 Admin

Der Bereich **Admin** stellt die Hauptkomponente zur Konfiguration von ESET Remote Administrator dar. Dieser Bereich enthält alle Tools, die dem Administrator zur Verwaltung der Client-Sicherheitslösungen und der ERA-Servereinstellungen zur Verfügung stehen. Mit den Tools im Bereich „Admin“ können Sie die Netzwerkumgebung so konfigurieren, dass keine umständliche Wartung erforderlich ist. Außerdem können Sie Benachrichtigungen und Dashboards konfigurieren, die Sie über den Netzwerkstatus auf dem Laufenden halten.

In diesem Abschnitt

- Dynamische Gruppen-Templates
- Gruppen
- Policies
- Client-Tasks
- Server-Tasks
- Trigger
- Benachrichtigungen
- Peerzertifikate
- Zugriffsrechte
- Servereinstellungen
- Lizenzverwaltung

6.1.1 Gruppen

Mit Gruppen können Sie Computer verwalten und in Kategorien einordnen. Anschließend können Sie auf Grundlage der Gruppenmitgliedschaft ganz einfach verschiedene Einstellungen, Tasks oder Einschränkungen auf die Clientcomputer anwenden. Sie können vordefinierte Gruppen und Gruppen-Templates verwenden oder neue erstellen.

Es gibt zwei Haupttypen für Clientgruppen:

Statische Gruppen

Statische Gruppen sind Gruppen ausgewählter Clientcomputer (Mitglieder). Die Gruppenmitglieder sind statisch und können nur manuell und nicht auf Grundlage dynamischer Kriterien hinzugefügt/entfernt werden. Ein Computer kann jeweils nur in einer statischen Gruppe enthalten sein.

Dynamische Gruppen

Dynamische Gruppen sind Gruppen aus Clients, deren Mitgliedschaft in der Gruppe nach bestimmten Kriterien festgelegt wird. Wenn ein Client die Kriterien nicht erfüllt, wird er aus der Gruppe entfernt. Computer, die die Kriterien erfüllen, werden automatisch zur Gruppe hinzugefügt.

Das Fenster **Gruppen** ist in drei Abschnitte unterteilt:

1. Links wird eine Liste aller Gruppen und ihrer Untergruppen angezeigt. Sie können eine Gruppe und eine Aktion für diese Gruppe aus dem Kontextmenü auswählen (Zahnradsymbol neben dem Gruppennamen). Die Optionen sind die gleichen wie die unten beschriebenen (Schaltfläche für Gruppenaktionen).

2. Im rechten Bereich werden Details zur ausgewählten Gruppe angezeigt (Sie können zwischen den Registerkarten navigieren):

- **Computer**, die Mitglied der Gruppe sind.
- **Policies**, die der Gruppe zugewiesen sind.
- **Tasks**, die der Gruppe zugewiesen sind.
- **Zusammenfassung**, eine kurze Beschreibung der Gruppe.

3. Über die Schaltflächen des Pop-up-Menüs **Gruppen** und **Computer** können Sie folgende Aktionen ausführen:

Gruppen-Aktionsschaltfläche

+ Neue statische Gruppe ...
Diese Option wird verfügbar, wenn Sie links in der Liste auf eine **Gruppe** klicken. Diese Gruppe ist dann die standardmäßige übergeordnete Gruppe. Sie können dies übergeordnete Gruppe jedoch später beim Erstellen einer neuen statischen Gruppe ändern.

+ Neue dynamische Gruppe ...
Diese Option wird verfügbar, wenn Sie links in der Liste auf eine **Gruppe** klicken. Diese Gruppe ist dann die standardmäßige übergeordnete Gruppe. Sie können dies übergeordnete Gruppe jedoch später beim Erstellen einer neuen dynamischen Gruppe ändern.

Bearbeiten ...
Hier können Sie die ausgewählte Gruppe bearbeiten. Es gelten die gleichen Einstellungen wie beim Erstellen einer neuen (statischen oder dynamischen) Gruppe.

Verschieben ...
Sie können eine Gruppe auswählen und als Untergruppe einer anderen Gruppe verschieben.

Löschen
Entfernt die ausgewählte Gruppe vollständig.

Importieren ...
Sie können eine Liste (üblicherweise eine Textdatei) von Computern, die Mitglied der ausgewählten Gruppe werden sollen, importieren. Wenn die Computer bereits in der Gruppe vorhanden sind, wird der Konflikt je nach ausgewählter Aktion aufgelöst:

- **Computer mit Konflikten überspringen** (Computer mit Konflikten werden nicht hinzugefügt)
- **Computer mit Konflikten aus anderen Gruppen verschieben** (Computer mit Konflikten werden aus anderen Gruppen, in denen sie enthalten sind, hierher verschoben)
- **Computer mit Konflikten duplizieren** (Computer mit Konflikten werden mit einem anderen Namen hinzugefügt).

Exportieren ...
Exportieren Sie die Mitglieder der Gruppe (und Untergruppen, sofern ausgewählt) als Liste (*TXT*-Datei). Die Liste kann zur Überprüfung verwendet oder später wieder importiert werden.

+ Neue hinzufügen ...
Mit dieser Option können Sie ein neues Gerät hinzufügen.

Scannen
Mit dieser Option wird der Task On-Demand-Scan auf dem Client ausgeführt, der die Bedrohung gemeldet hat.

Update der Signaturdatenbank
Mit dieser Option wird der Task Update der Signaturdatenbank ausgeführt (löst manuell ein Update aus).

Mobilgerät

- **Registrieren ...** Mit dieser Option können Sie einen neuen Clienttask erstellen.
- **Suchen** – Zum Anfordern der GPS-Koordinaten des Mobilgeräts.
- **Sperren** – Das Gerät wird gesperrt, wenn eine verdächtige Aktivität erkannt oder das Gerät als „vermisst“ gekennzeichnet wird.
- **Entsperren** – Das Gerät wird entsperrt.
- **Alarm** – Löst remote einen lauten Alarm aus. Der Alarm wird auch ausgelöst, wenn das Gerät stumm geschaltet ist.
- **Daten löschen** – Alle auf dem Gerät gespeicherten Daten werden dauerhaft gelöscht.

+ Neuer Task ...

Mit dieser Option können Sie einen neuen Clienttask erstellen. Wählen Sie einen Task aus und konfigurieren Sie (optional) die Drosselung für den Task. Der Task wird gemäß den Taskeinstellungen in die Warteschlange gesetzt. Diese Option löst sofort einen vorhandenen Task aus, den Sie aus einer Liste der verfügbaren Tasks auswählen. Für diesen Task ist der Trigger nicht verfügbar, weil er sofort ausgeführt wird.

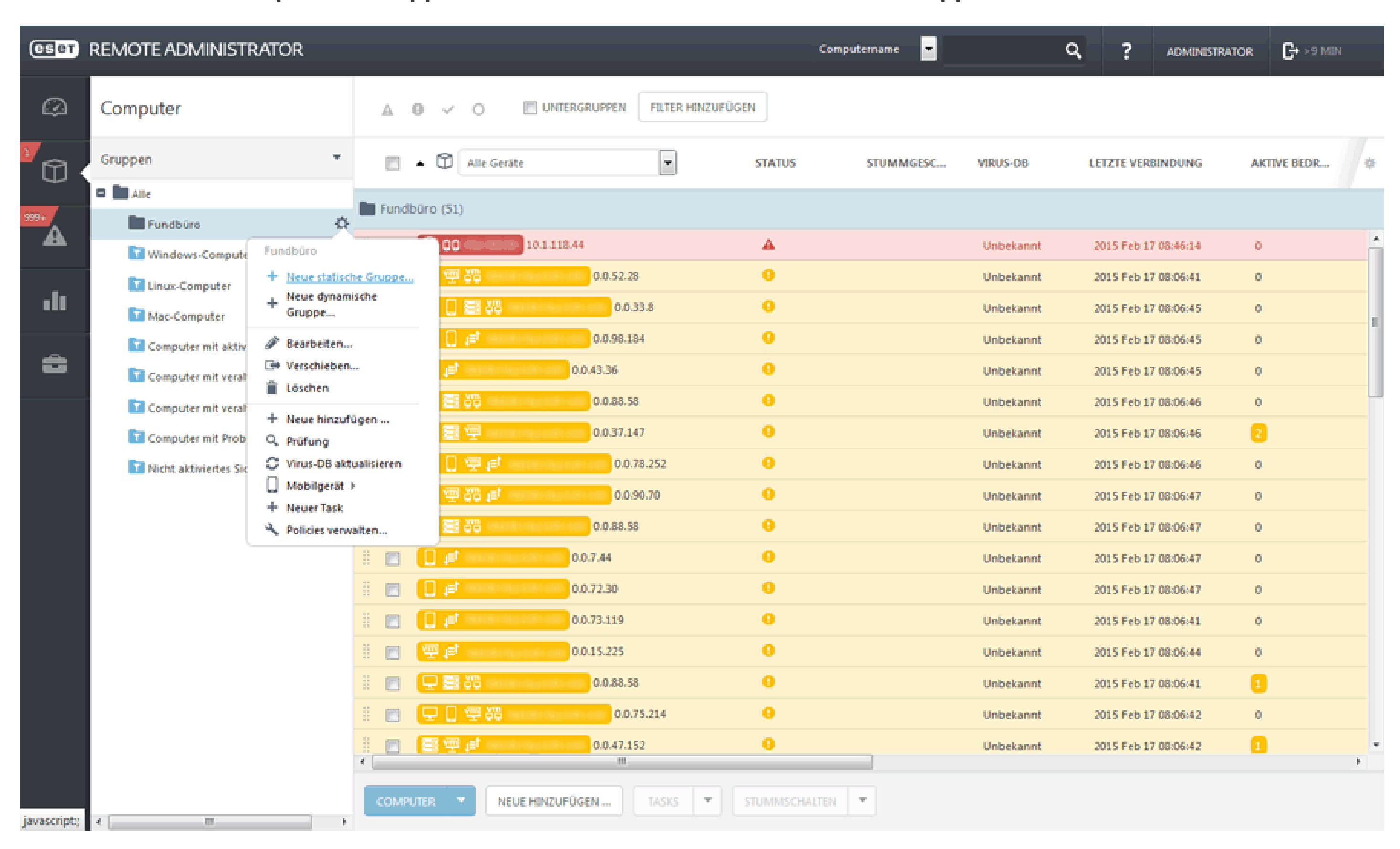
Policies verwalten ...

Weisen Sie einer ausgewählten Gruppe eine Policy zu.

6.1.1.1 Neue statische Gruppe erstellen

Zum Erstellen einer neuen statischen Gruppe stehen drei Methoden zur Auswahl:

1. Klicken Sie auf **Computer** > **Gruppen** > ⚙ und wählen Sie **Neue statische Gruppe** aus.

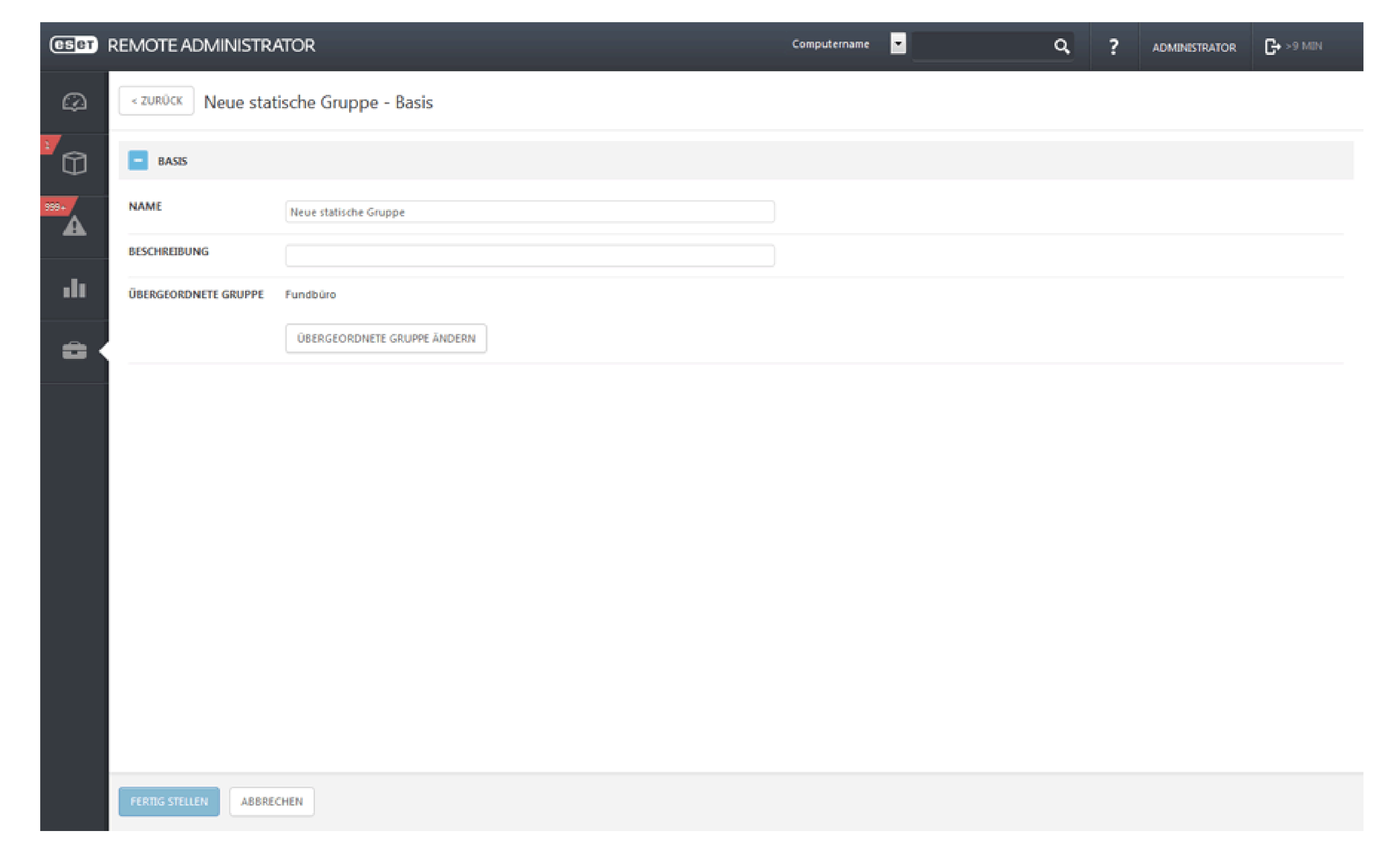


2. Klicken Sie auf **Admin** > **Gruppen** > ⚙ > **Neue statische Gruppe ...**.

3. Klicken Sie auf **Admin** > **Gruppen**, wählen Sie eine statische Gruppe aus und klicken Sie auf **Gruppe**.

Basis

Geben Sie einen **Namen** und eine **Beschreibung** (optional) für die neue statische Gruppe ein. Standardmäßig ist die übergeordnete Gruppe die Gruppe, die Sie zu Beginn des Erstellungsvorgangs der neuen statischen Gruppe ausgewählt haben. Wenn Sie die übergeordnete Gruppe ändern möchten, klicken Sie auf **Übergeordnete Gruppe ändern** und wählen Sie aus der Baumstruktur eine übergeordnete Gruppe aus. Die übergeordnete Gruppe der neuen statischen Gruppe muss eine statische Gruppe sein. Dynamische Gruppen dürfen keine statischen Gruppen enthalten. Klicken Sie auf **Fertig stellen**, um die neue statische Gruppe zu erstellen.



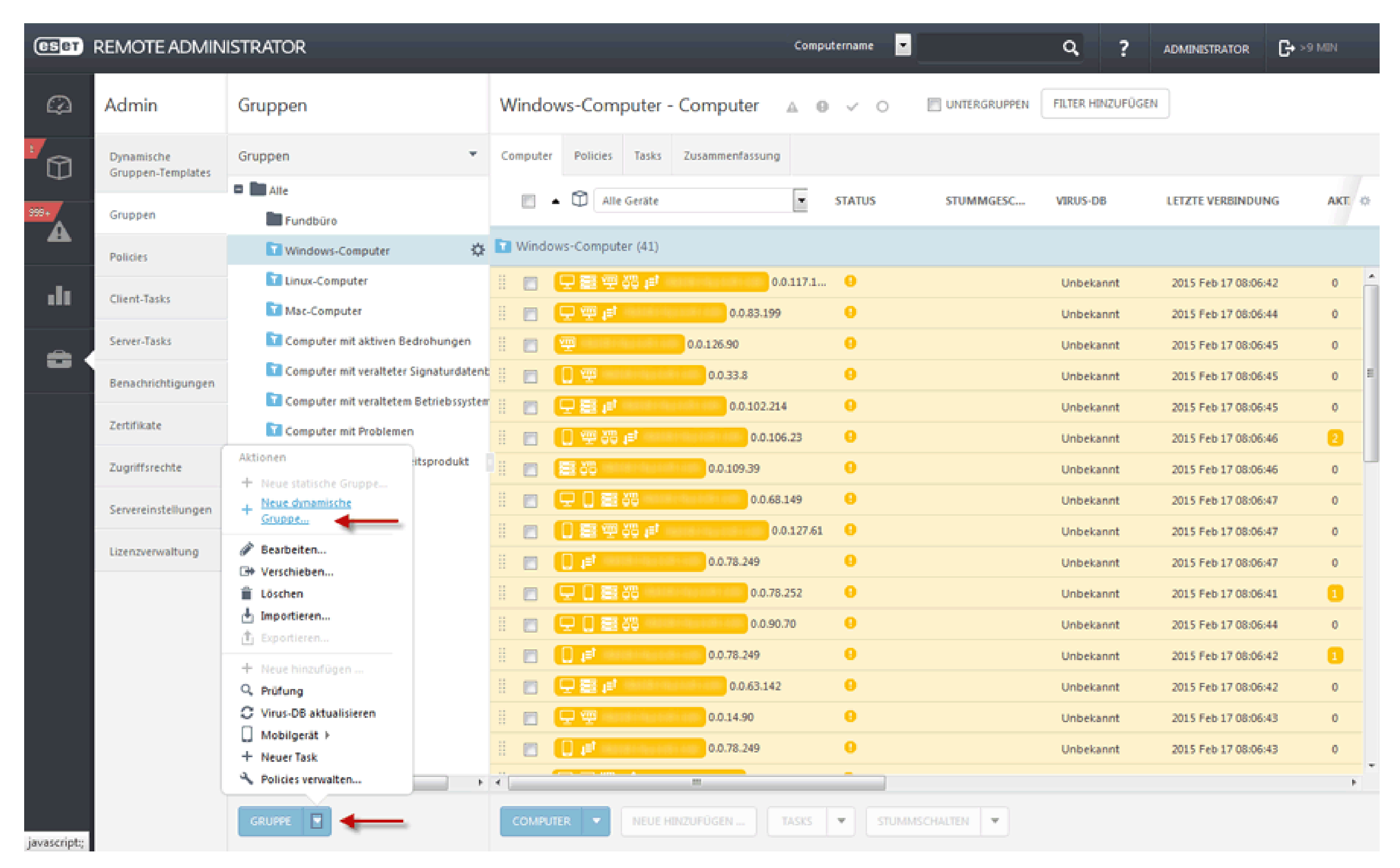
6.1.1.2 Erstellen einer neuen dynamischen Gruppe

Zum Erstellen einer neuen dynamischen Gruppe stehen drei Methoden zur Auswahl:

1. Klicken Sie auf **Computer** > **Gruppen** > ⚙ und anschließend auf **Neue dynamische Gruppe...**

2. Klicken Sie auf **Admin** > **Gruppen** > ⚙ > **Neue dynamische Untergruppe ....**

3. Klicken Sie auf **Admin** > **Gruppen**, klicken Sie anschließend auf die Schaltfläche **Gruppe** und auf **Neue dynamische Gruppe...**



Der Assistent für neue dynamische Gruppen wird angezeigt.

6.1.1.3 Zuweisen eines Task zu einer Gruppe

Klicken Sie auf **Admin** > **Gruppen**, wählen Sie eine **Statische** oder **Dynamische** Gruppe aus ⚙ neben der ausgewählten Gruppe. Klicken Sie alternativ auf **Gruppe** > **+ Neuer Task**

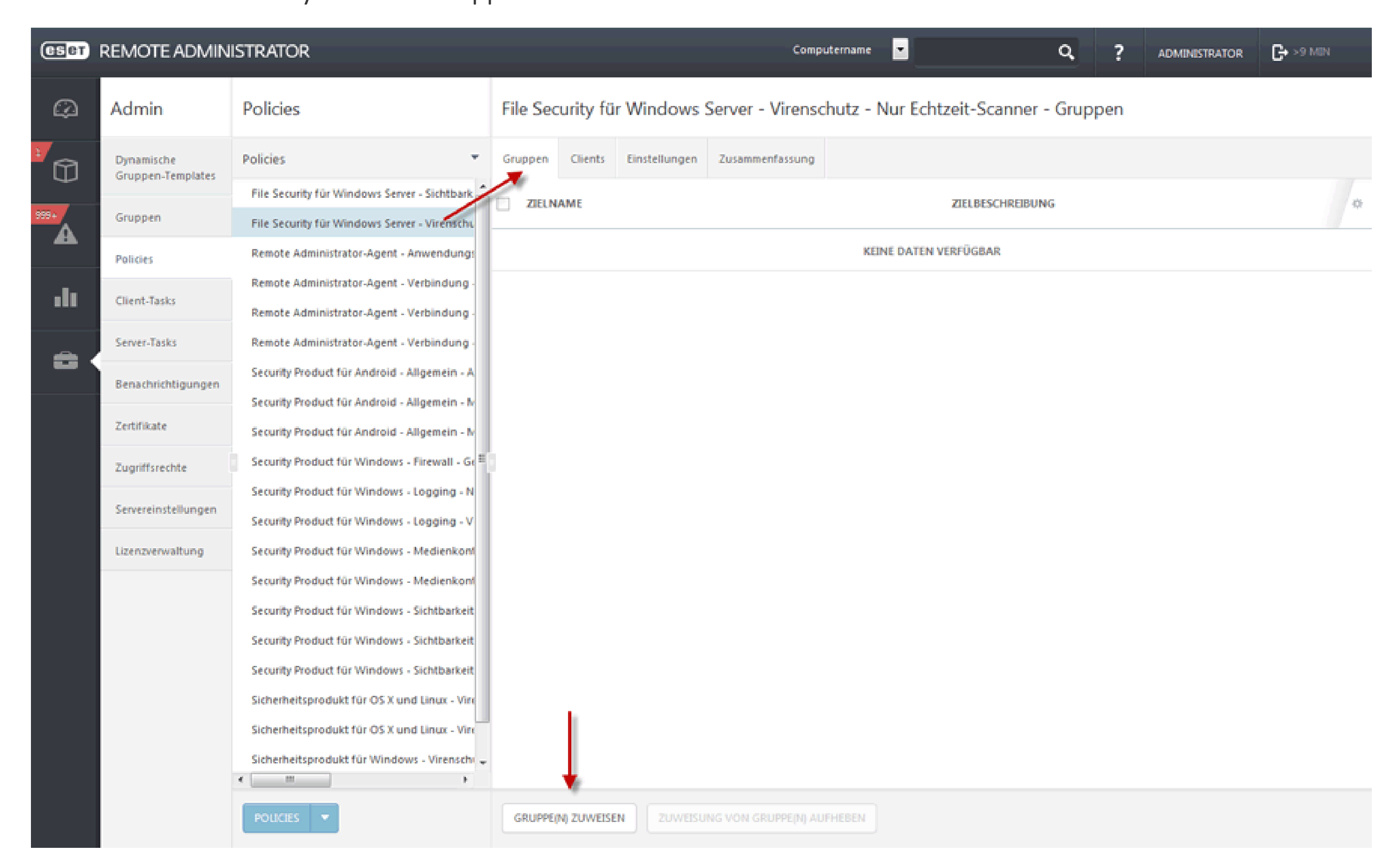
Sie können auch unter **Computer** eine **Statische** oder **Dynamische** Gruppe auswählen und auf ⚙ > **+ Neuer Task** klicken.

Der Assistent für neue Client-Tasks wird geöffnet.

6.1.1.4 Zuweisen einer Policy zu einer Gruppe

Nachdem Sie eine Policy erstellt haben, können Sie sie einer **statischen** oder **dynamischen Gruppe** zuweisen. Es gibt zwei Möglichkeiten zum Zuweisen einer Policy:

1. Klicken Sie auf **Admin** > **Policies**, wählen Sie eine Policy aus und klicken Sie auf **Gruppe(n) zuweisen**. Wählen Sie eine statische oder dynamische Gruppe aus und klicken Sie auf **OK**.



Wählen Sie **Gruppe** in der Liste aus.

2. Klicken Sie auf **Admin** > **Gruppen** > **Gruppe** oder neben dem Gruppennamen auf das Zahnradsymbol ⚙. Wählen Sie **Policies** verwalten aus.

Klicken Sie im Fenster **Anwendungsreihenfolge für Policies** auf **Policy hinzufügen**. Aktivieren Sie das Kontrollkästchen neben der Policy, die Sie der Gruppe zuweisen möchten, und klicken Sie auf **OK**.
Klicken Sie auf **Speichern**. Um anzuzeigen, welche Policies einer bestimmten Gruppe zugewiesen sind, wählen Sie die gewünschte Gruppe aus und klicken Sie auf die Registerkarte **Policies**. Eine Liste der Policies, die dieser Gruppe zugewiesen sind, wird angezeigt.

HINWEIS: Weitere Informationen zu Policies finden Sie im Kapitel Policies.

6.1.1.5 Policies und Gruppen

Die Mitgliedschaft eines Computers in einer dynamischen Gruppe wird über Policies festgelegt, die dem Computer zugewiesen sind. Zum Festlegen der Mitgliedschaft wird außerdem das Template verwendet, auf dem die dynamische Gruppe basiert.

6.1.1.6 Statische Gruppen

- Statische Gruppen dienen dem manuellen Ordnen der Clientcomputer in **Gruppen** und **Untergruppen**. Sie können benutzerdefinierte statische Gruppen erstellen und die gewünschten Computer in diese Gruppen verschieben.
- Statische Gruppen können nur manuell erstellt werden. Anschließend können Clientcomputer manuell in diese Gruppen verschoben werden. Jeder Computer kann stets nur zu einer statischen Gruppe gehören.

Es gibt zwei standardmäßige statische Gruppen:

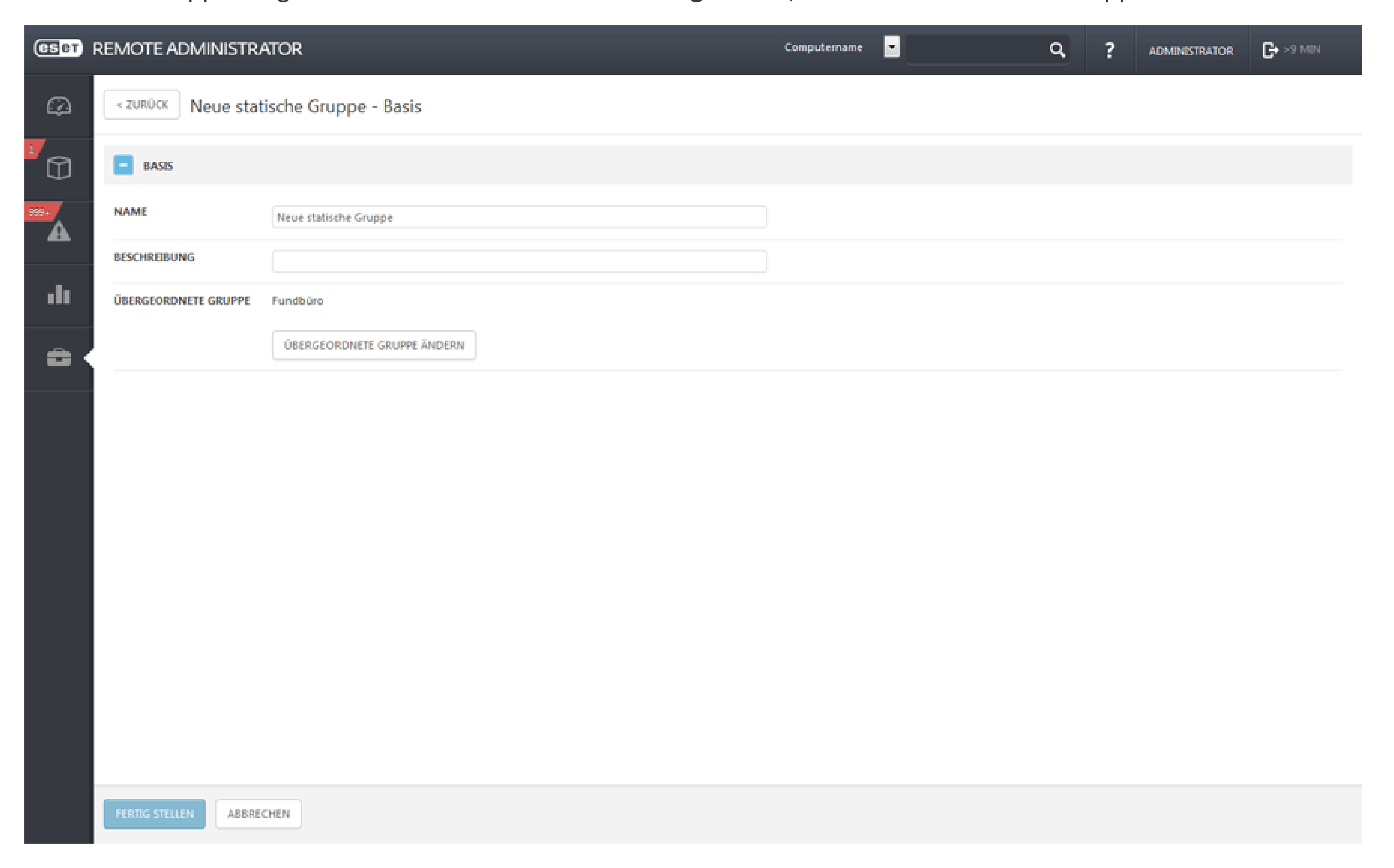
- **Alle –** Dies ist eine Hauptgruppe für alle Computer im Netzwerk des ERA-Servers. Über diese Gruppe werden die Policies auf jeden Computer als standardmäßige Policy angewendet. Die Gruppe wird immer angezeigt und ihr Name kann nicht geändert werden.
- **Fundbüro** als Untergruppe der Gruppe **Alle** – Bei der ersten Verbindung zwischen Agent und Server wird jeder neue Computer zunächst automatisch in dieser Liste angezeigt. Die Gruppe kann umbenannt und kopiert werden, jedoch nicht gelöscht oder verschoben.

6.1.1.6.1 Assistent für statische Gruppen

Wählen Sie unter **Computer** > **Gruppen** eine der statischen Guppen aus und klicken Sie auf das Zahnradsymbol ⚙. Wählen Sie dann **Neue statische Gruppe** aus.

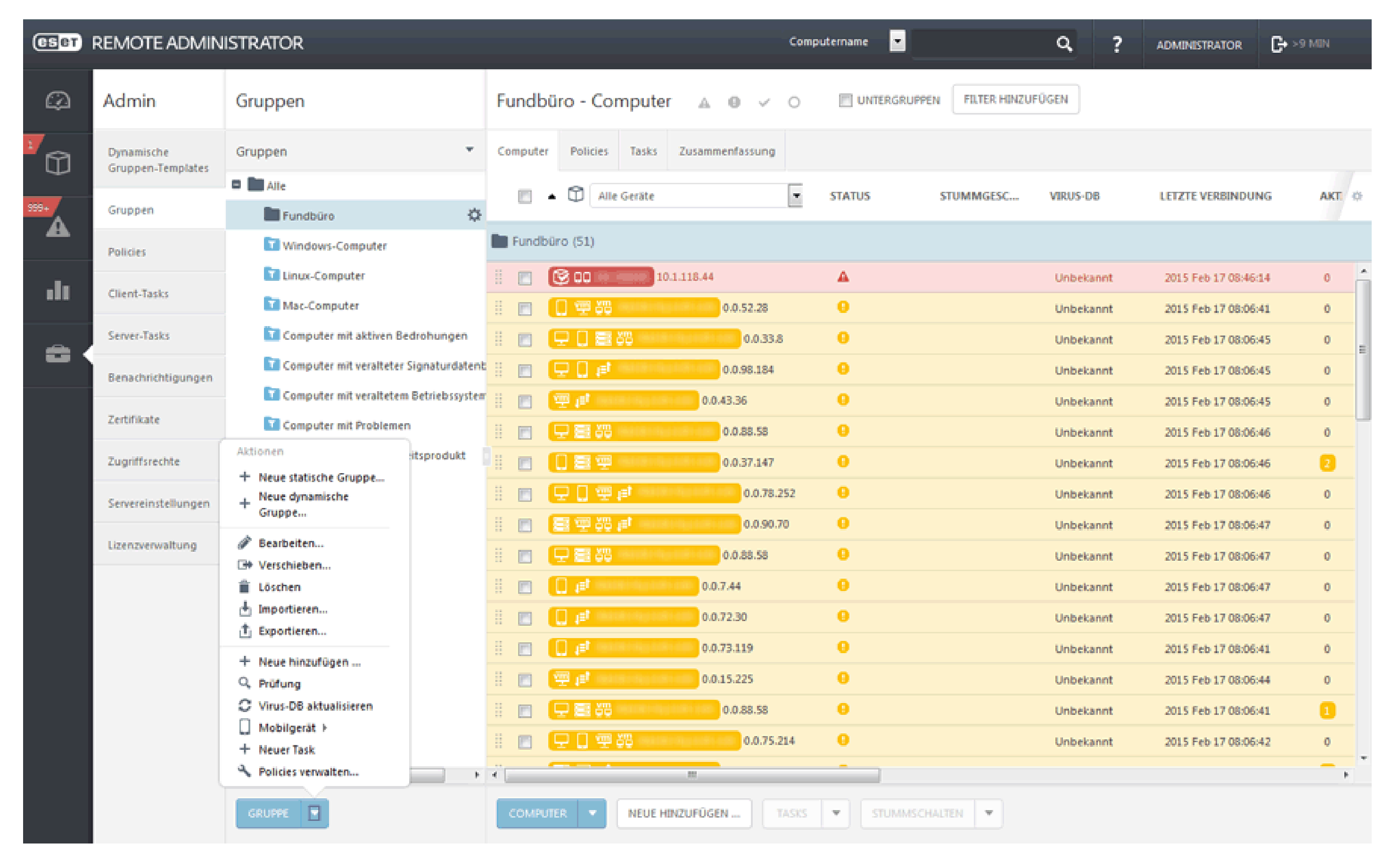
Basis

Geben Sie einen **Namen** und eine **Beschreibung** für die neue Gruppe ein. Optional können Sie die **übergeordnete Gruppe** ändern. Standardmäßig ist die übergeordnete Gruppe diejenige Gruppe, die Sie beim Erstellen der statischen Gruppe ausgewählt haben. Klicken Sie auf **Fertig stellen**, um die neue statische Gruppe zu erstellen.



6.1.1.6.2 Verwalten statischer Gruppen

Navigieren Sie zu **Admin** > **Gruppen** > und wählen Sie die statische Gruppe aus, die Sie verwalten möchten. Klicken Sie auf die Schaltfläche **Gruppe** oder auf das Zahnradsymbol ⚙ neben dem Namen der statischen Gruppe. Ein Pop-up-Menü mit den verfügbaren Optionen wird angezeigt:



Neue statische Gruppe

Die statische Gruppe, die Sie beim Klicken auf die Schaltfläche **Gruppe** oder auf das Zahnradsymbol ⚙ ausgewählt haben, wird als standardmäßige übergeordnete Gruppe verwendet. Sie können die übergeordnete Gruppe jedoch später (je nach Bedarf) ändern, wenn Sie eine neue statische Gruppe erstellen.

Gruppe bearbeiten

Hier können Sie die ausgewählte Gruppe bearbeiten. Es gelten die gleichen Einstellungen wie beim Erstellen einer neuen (statischen oder dynamischen) Gruppe.

Verschieben

Mit dieser Option können Sie die ausgewählte Gruppe in eine andere Gruppe verschieben. Die verschobene Gruppe wird eine Untergruppe der Gruppe, in die sie verschoben wurde.

Löschen

Entfernt die ausgewählte Gruppe vollständig.

Exportieren

Exportieren Sie die Mitglieder der Gruppe (und Untergruppen, sofern ausgewählt) als Liste (*TXT*-Datei). Die Liste kann zur Überprüfung verwendet oder später wieder importiert werden.

Importieren

Sie können eine Liste (üblicherweise eine Textdatei) von Computern, die Mitglied der ausgewählten Gruppe werden sollen, importieren.

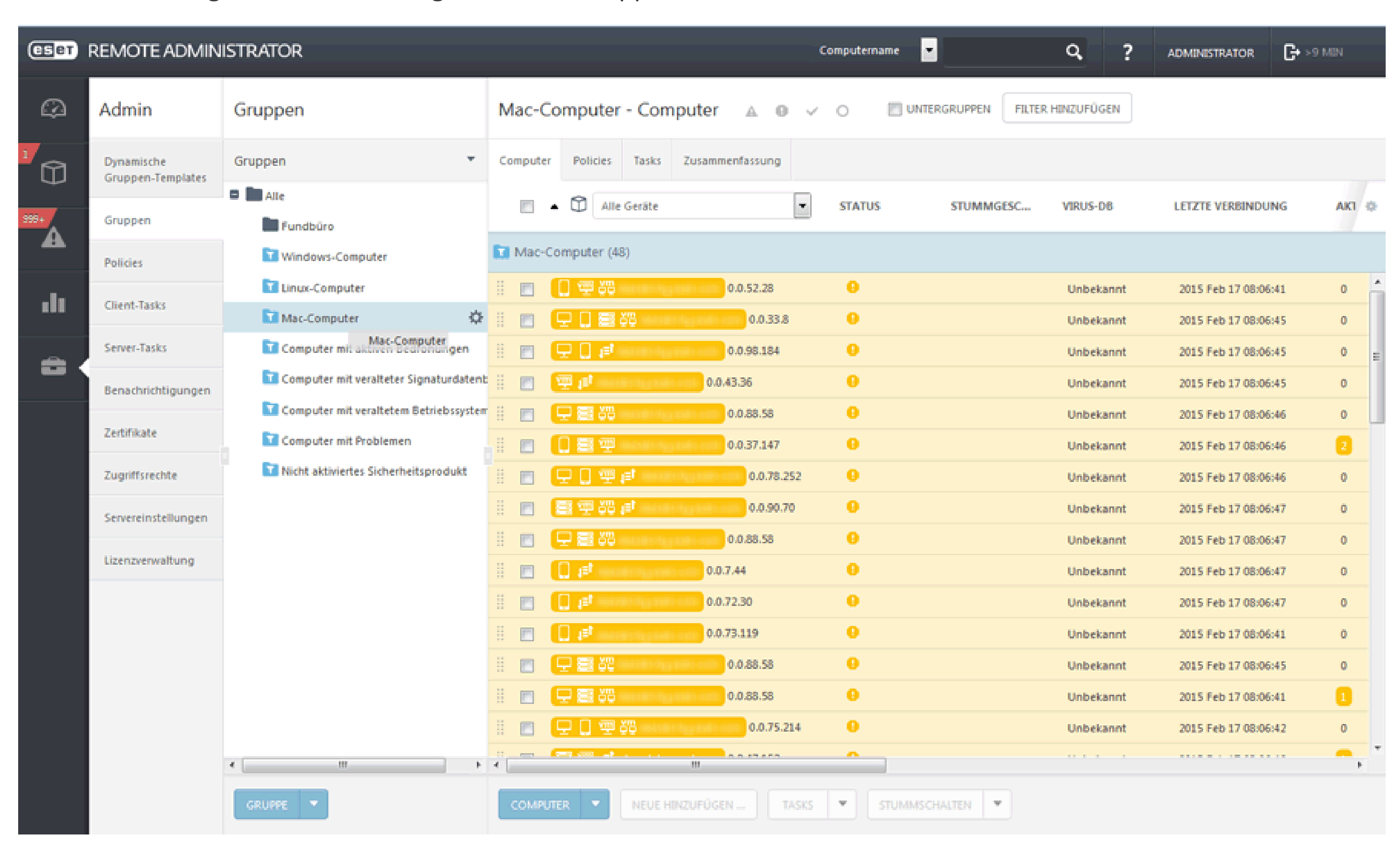
6.1.1.6.3 Verschieben einer statischen Gruppe

Klicken Sie auf das Zahnradsymbol neben dem Gruppennamen und wählen Sie **Verschieben** aus. Ein Pop-up-Fenster mit der Baumstruktur der Gruppen wird angezeigt. Wählen Sie die (statische oder dynamische) Zielgruppe aus, in die Sie die ausgewählte Gruppe verschieben möchten. Die Zielgruppe wird eine übergeordnete Gruppe. Sie können eine Gruppe auch durch Ziehen der Gruppe und Ablegen in der gewünschten Zielgruppe verschieben.

Einige Ausnahmen bei der Gruppenorganisation müssen beachtet werden. **Eine statische Gruppe kann nicht in eine dynamische Gruppe** verschoben werden. Außerdem können keine vordefinierten statischen Gruppen (zum Beispiel die Gruppe „Fundbüro“) in eine andere Gruppe verschoben werden. Andere Gruppen können frei verschoben werden. Eine dynamische Gruppe kann Mitglied einer beliebigen anderen Gruppe sein, auch einer statischen Gruppe.

Zum Verschieben von Gruppen stehen folgende Methoden zur Verfügung:

Ziehen und Ablegen - Klicken Sie auf die zu verschiebende Gruppe und halten Sie die Maustaste gedrückt. Bewegen Sie den Mauszeiger zur neuen übergeordneten Gruppe Ihrer Wahl und lassen Sie die Maustaste los.



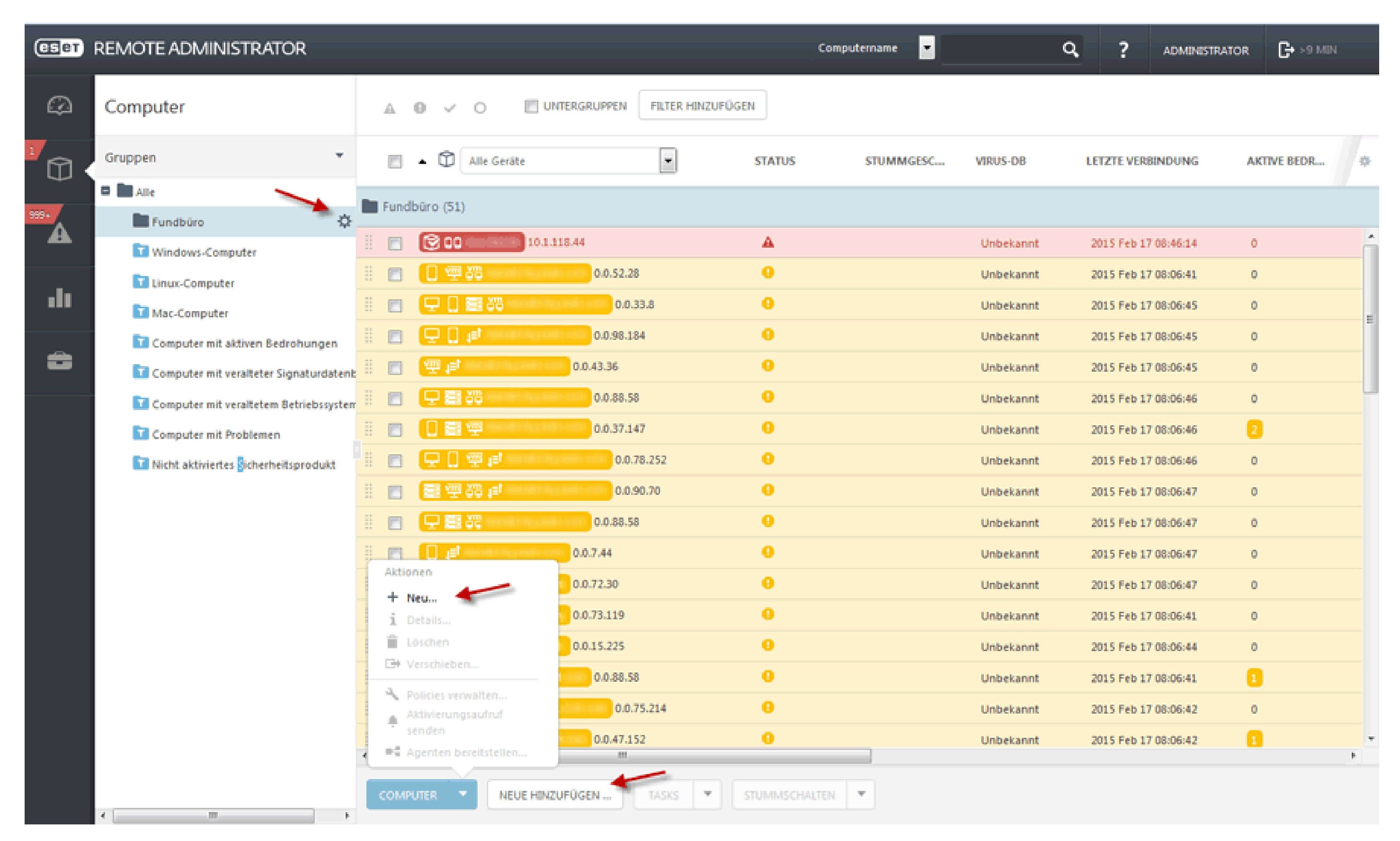
> **Bearbeiten** > **Übergeordnete Gruppe ändern**.

⚙ > **Verschieben** > Auswahl einer neuen übergeordneten Gruppe aus der Liste und Klicken auf **OK**.

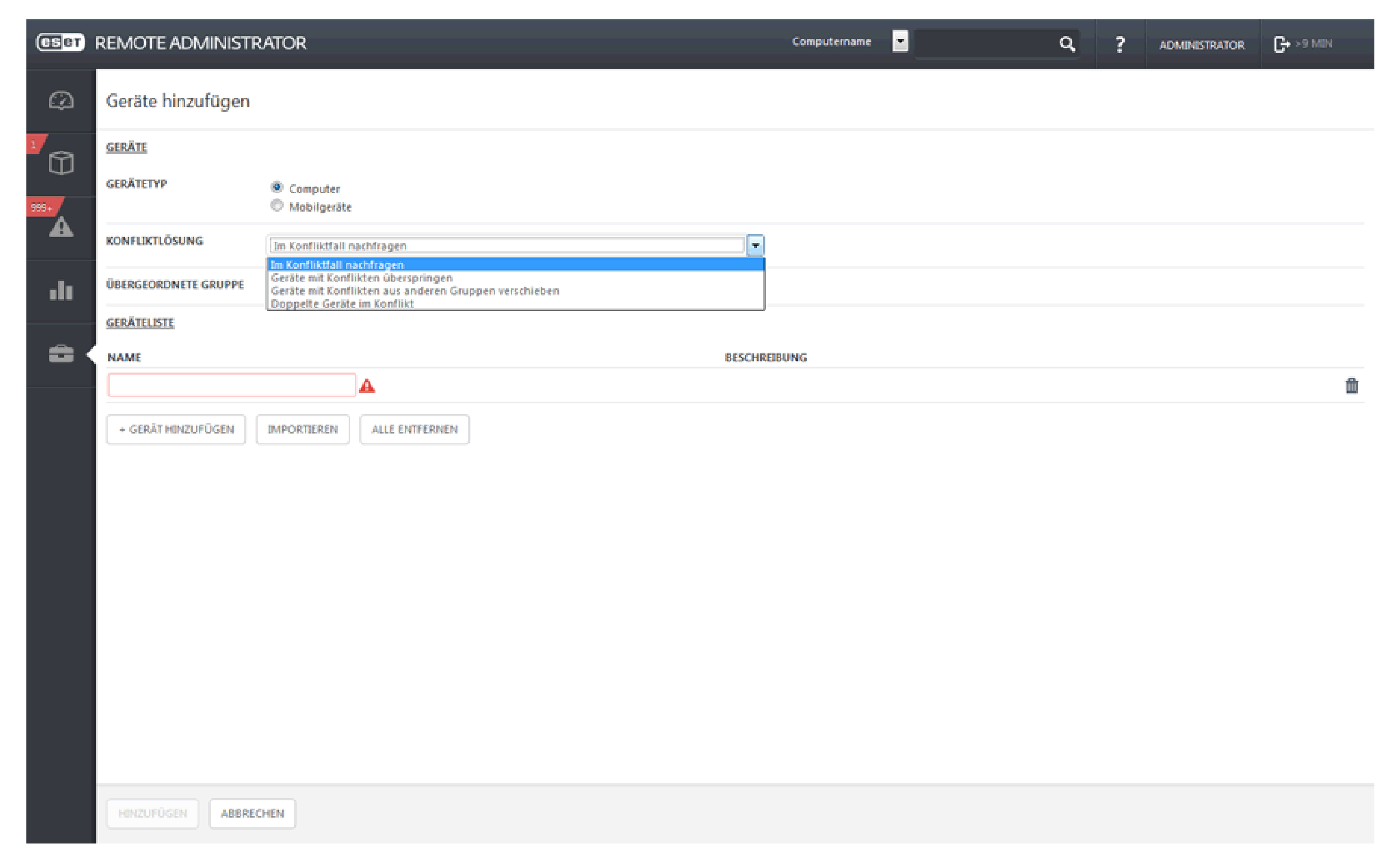
6.1.1.6.4 Hinzufügen eines Clientcomputers zu einer statischen Gruppe

Erstellen Sie eine neue statische Gruppe oder wählen Sie eine der standardmäßigen statischen Gruppen aus.

Die **Registerkarte** Computer bietet drei Möglichkeiten zum Hinzufügen neuer Computer. Wählen Sie beispielsweise eine statische Gruppe aus, klicken Sie auf das Zahnradsymbol ⚙ und wählen Sie **+ Neue hinzufügen** aus.



Geben Sie den Namen des hinzuzufügenden Computers in das Feld **Name** ein. Klicken Sie auf + Gerät hinzufügen, um zusätzliche Computer hinzuzufügen, oder klicken Sie auf Importieren, um eine Datei mit einer Liste der hinzuzufügenden Computer zu importieren. Wahlweise können Sie eine **Beschreibung** für die Computer eingeben.



Im Dropdown-Menü „Konfliktlösung“ können Sie eine Aktion für den Fall auswählen, dass der Computer bereits in ERA vorhanden ist:

Im Konfliktfall nachfragen: Wenn ein Konflikt erkannt wird, fordert das Programm Sie zur Auswahl einer Aktion auf (siehe nachstehende Optionen).
Computer mit Konflikten überspringen: Bereits vorhandene Computer werden nicht hinzugefügt.
Computer mit Konflikten aus anderen Gruppen verschieben: Computer mit Konflikten werden aus der ursprünglichen Gruppe in die Gruppe **Alle** verschoben.
Computer mit Konflikten duplizieren: Neue Computer werden hinzugefügt, jedoch mit einem anderen Namen.

Klicken Sie auf **Hinzufügen**. Wenn Sie eine Gruppe auswählen, werden rechts in der Liste die zur Gruppe gehörenden Computer angezeigt.

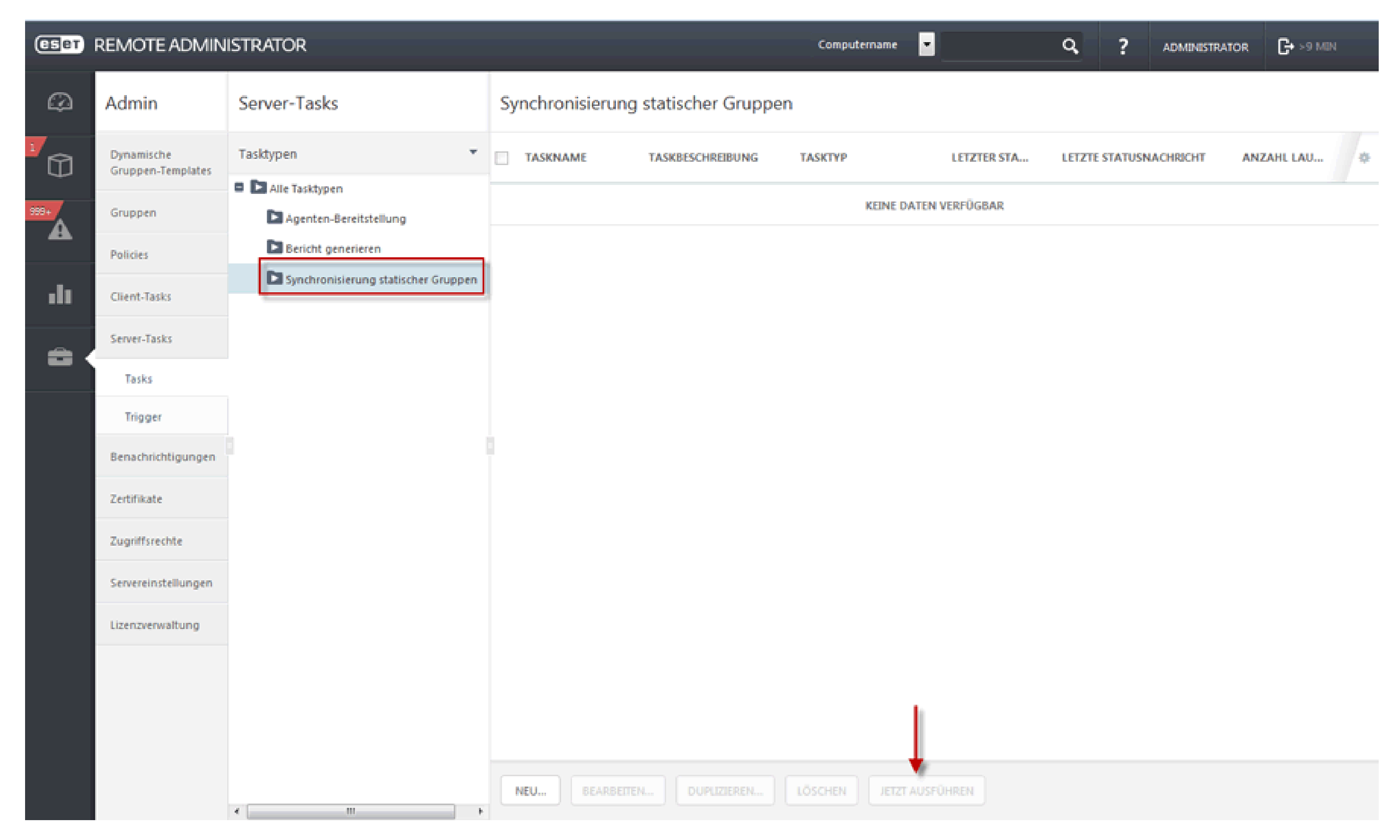
HINWEIS: Das Hinzufügen mehrerer Computer kann einige Zeit in Anspruch nehmen, Reverse-DNS-Lookup kann durchgeführt werden.

Weitere Informationen zum Hinzufügen von Mobilgeräten finden Sie im Kapitel Mobilgeräteregistrierung.

6.1.1.6.5 Importieren von Clients aus Active Directory

Die AD-Synchronisierung wird über den Servertask **Synchronisierung statischer Gruppen** ausgeführt.

Admin > **Servertask** ist ein vordefinierter Standardtask, den Sie während der Installation von ESET Remote Administrator automatisch ausführen lassen können. Wenn sich der Computer in einer Domäne befindet, wird die Synchronisierung ausgeführt und die Computer aus AD in der Standardgruppe **Alle** aufgelistet.



Klicken Sie auf den Task und wählen Sie **Jetzt ausführen** aus, um den Synchronisierungsvorgang zu starten. Wenn Sie einen neuen AD-Synchronisierungstask erstellen möchten, wählen Sie eine Gruppe aus, zu der Sie neue Computer aus AD hinzufügen möchten. Wählen Sie die Objekte im AD aus, von denen Sie synchronisieren möchten, und wählen Sie Aktionen für Duplikate aus. Geben Sie die Verbindungseinstellungen für den AD-Server ein und legen Sie den **Synchronisierungsmodus** auf **Active Directory/Open Directory/LDAP** fest.

Weitere Informationen finden Sie in diesem ESET Knowledgebase-Artikel.

6.1.1.6.6 Zuweisen eines Tasks zu einer statischen Gruppe

In Bezug auf die Zuweisung von Tasks werden statische und dynamische Gruppen gleich behandelt. Anweisungen zum Zuweisen eines Tasks zu einer Gruppe finden Sie hier.

6.1.1.6.7 Zuweisen einer Policy zu einer statischen Gruppe

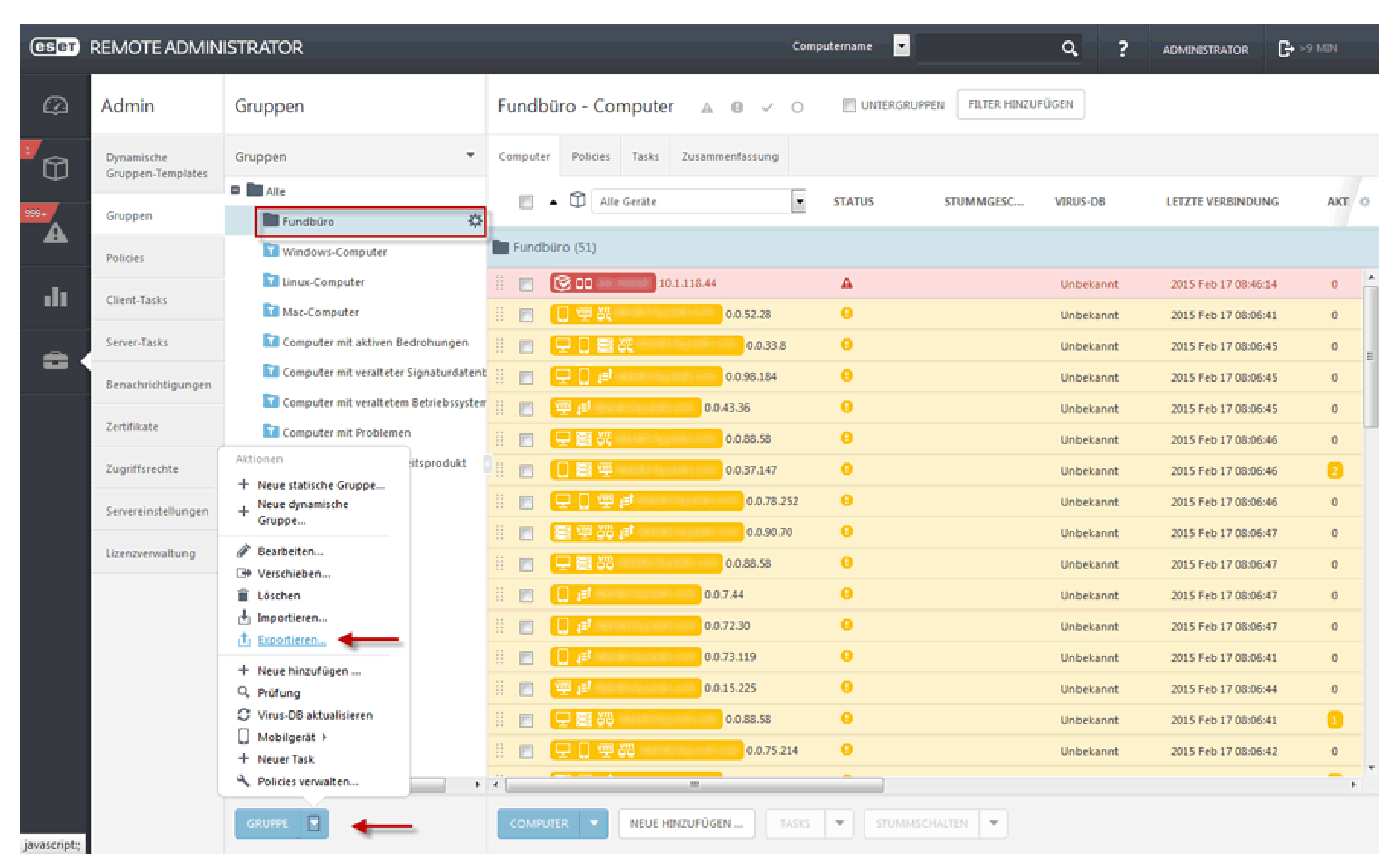
In Bezug auf die Zuweisung von Policies werden statische und dynamische Gruppen gleich behandelt. Anweisungen zum Zuweisen einer Policy zu einer Gruppe finden Sie hier.

6.1.1.6.8 Exportieren statischer Gruppen

Die Liste der Computer in der ERA-Struktur kann auf einfache Weise exportiert werden. Sie können die Liste exportieren und als Sicherung speichern. So steht zum späteren Import zur Verfügung, falls Sie beispielsweise die Gruppenstruktur wiederherstellen möchten.

HINWEIS: Eine statische Gruppe muss mindestens einen Computer enthalten. Leere Gruppen können nicht exportiert werden.

1. Navigieren Sie zu **Admin** > **Gruppen** > und wählen Sie die statische Gruppe aus, die Sie exportieren möchten.



2. Klicken Sie unten auf die Schaltfläche **Gruppe** (ein Kontextmenü wird geöffnet).

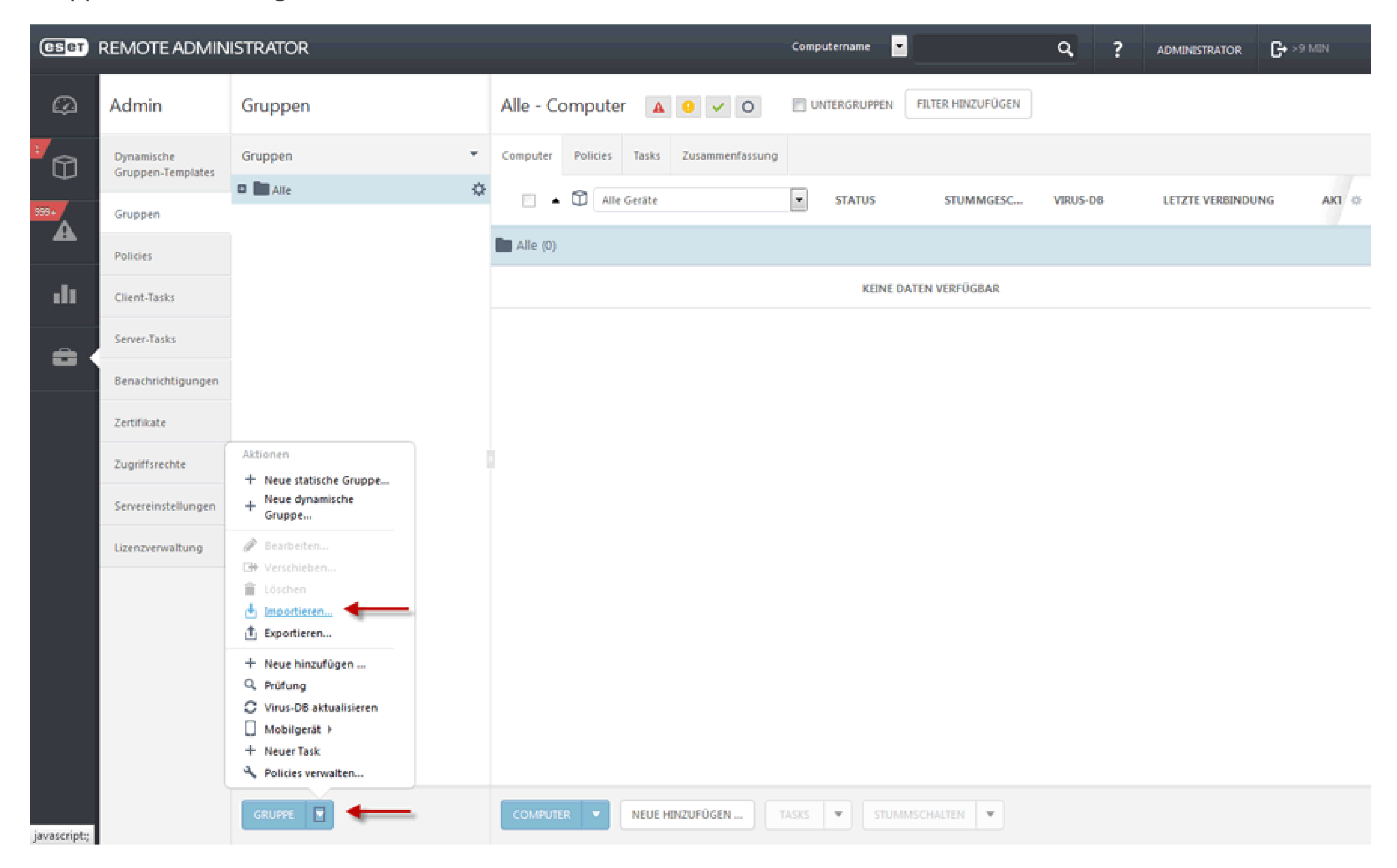
3. Wählen Sie **Exportieren aus.**

4. Die Datei wird im **TXT**-Format gespeichert.

HINWEIS: Dynamische Gruppen können nicht exportiert werden, weil es sich hierbei nur um Verknüpfungen zu Computern handelt, welche die in den Vorlagen für dynamische Gruppen definierten Kriterien erfüllen.

6.1.1.6.9 Importieren statischer Gruppen

Exportierte Dateien statischer Gruppen können zurück in die ERA Web-Konsole importiert und in die vorhanden Gruppenstruktur integriert werden.



1. Klicken Sie auf **Gruppe** (ein Kontextmenü wird geöffnet).
2. Wählen Sie **Importieren** aus.
3. Klicken Sie auf **Durchsuchen** und navigieren Sie zur **TXT**-Datei.
4. Wählen Sie die Datei der Gruppe aus und klicken Sie auf **Öffnen.** Der Dateiname wird im Textfeld angezeigt.
5. Wählen Sie für das Beheben von Konflikten eine der folgenden Optionen aus:

- **Computer mit Konflikten überspringen**
Wenn statische Gruppen vorhanden sind und ein Computer aus der TXT-Datei bereits in einer dieser Gruppen enthalten ist, wird der entsprechende Computer übersprungen und nicht importiert. Es wird eine entsprechende Information hierzu angezeigt.

- **Computer mit Konflikten aus anderen Gruppen verschieben**
Wenn statische Gruppen vorhanden sind und Computer aus der TXT-Datei bereits in einer dieser Gruppen vorhanden sind, müssen die Computer vor dem Importieren in eine andere statische Gruppe verschoben werden. Nach dem Importieren werden die Computer wieder in ihre ursprüngliche Gruppe zurückverschoben.

- **Computer mit Konflikten duplizieren**
Wenn statische Gruppen vorhanden sind und Computer aus der TXT-Datei bereits in einer dieser Gruppen enthalten sind, werden in der gleichen statischen Gruppe Duplikate dieser Computer erzeugt. Der ursprüngliche Computer wird mit den vollständigen Informationen und das Duplikat nur mit dem Computernamen angezeigt.

5. Klicken Sie auf **Importieren**. Die statischen Gruppen und die darin enthaltenen Computer werden importiert.

6.1.1.7 Dynamische Gruppen

Dynamische Gruppen sind im Grunde benutzerdefinierte Filter, die unter Templates definiert werden. Die Computer werden auf der Agentenseite gefiltert, sodass keine zusätzlichen Informationen an den Server übertragen werden müssen. Der Agent entscheidet selbst, zu welcher dynamischen Gruppe ein Client gehört, und benachrichtigt den Server lediglich über diese Entscheidung. Die Regeln für dynamische Gruppen sind im Template für dynamische Gruppen definiert.

Nach der Installation von ESET Remote Administrator stehen einige vordefinierte dynamische Gruppen zur Verfügung. Bei Bedarf können Sie benutzerdefinierte dynamische Gruppen erstellen. Wenn Sie eine benutzerdefinierte dynamische Gruppe erstellen möchten, erstellen Sie zuerst ein Template und erstellen Sie dann eine dynamische Gruppe.

Alternativ können Sie gleichzeitig eine neue dynamische Gruppe und ein neues Template erstellen.

Mit einem Template können mehrere dynamische Gruppen erstellt werden.

Ein Benutzer kann dynamische Gruppen in anderen Komponenten von ERA verwenden. Sie können der Gruppe Policies zuweisen oder einen Task für alle Computer in der Gruppe vorbereiten.

Dynamische Gruppen können sich unter statischen oder dynamischen Gruppen befinden. Die oberste Gruppe ist jedoch immer eine statische Gruppe.

Alle dynamischen Gruppen unter einer gegebenen statischen Gruppe filtern nur die Computer dieser statischen Gruppe, unabhängig davon, wie tief sie im Baum angeordnet sind. Bei verschachtelten dynamischen Gruppen filtert die tiefer gelegene dynamische Gruppe die Ergebnisse der darüber liegenden.

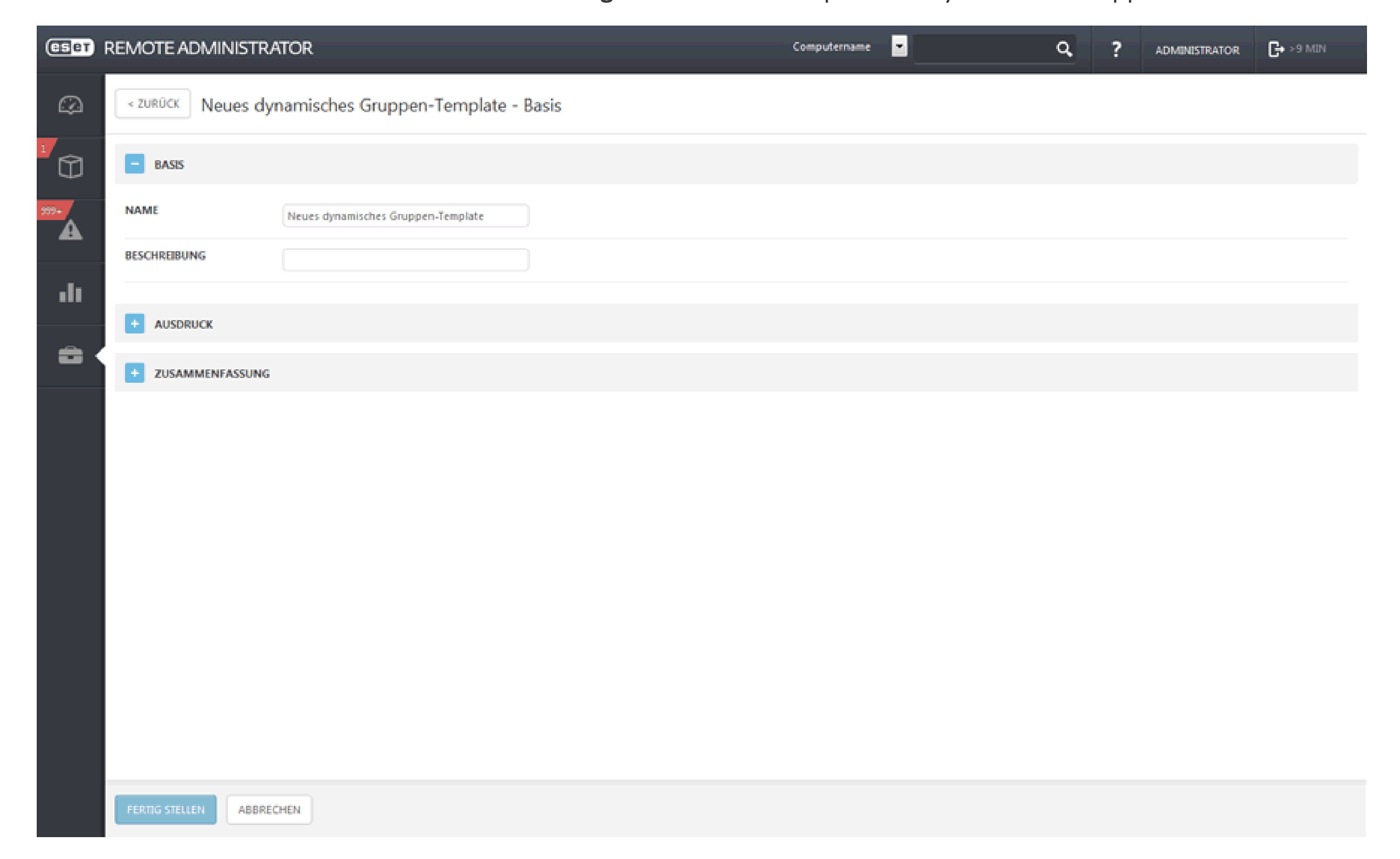
Nach der Erstellung können Sie jedoch frei im Baum verschoben werden.

6.1.1.7.1 Assistent für Templates für dynamische Gruppen

Klicken Sie auf **Neues Template** unter **Admin** > **Templates für dynamische Gruppen**.

Basis

1. Geben Sie einen **Namen** und eine **Beschreibung** für das neue Template für dynamische Gruppen ein.



Ausdruck

Wählen Sie einen logischen Operator im Menü **Operation** aus.

- **AND** – Alle festgelegten Bedingungen müssen erfüllt sein.
- **OR** – Mindestens eine Bedingung muss erfüllt sein.
- **NAND** – Mindestens eine Bedingung darf nicht erfüllt sein.
- **NOR** – Alle Bedingungen müssen falsch sein.

Wählen Sie beispielsweise **UND**. Dies bedeutet, dass der Computer alle Bedingungen erfüllen muss, um in der dynamischen Gruppe angezeigt zu werden, die dieses Template verwendet.

- Klicken Sie auf **+ Regel hinzufügen** und wählen Sie eine Bedingung aus. Nehmen wir an, Sie möchten Clients auswählen, die ein Notebook mit angeschlossenem Netzkabel verwenden. Wählen Sie **Hardware** > **Im Akkubetrieb** > **=(gleich)** > **Wird nicht entladen** aus.
- Klicken Sie auf **+ Regel hinzufügen**, um eine zweite Bedingung einzugeben (die Anzahl der Regeln ist unbegrenzt).Wählen Sie **Betriebssystemedition** > **OS-Typ** > **=(gleich)** > **Windows 8.1** (geben Sie diesen Wert in das leere Feld ein).

Wenn beide Bedingungen erfüllt sind, wird der Client in der dynamischen Gruppe angezeigt.

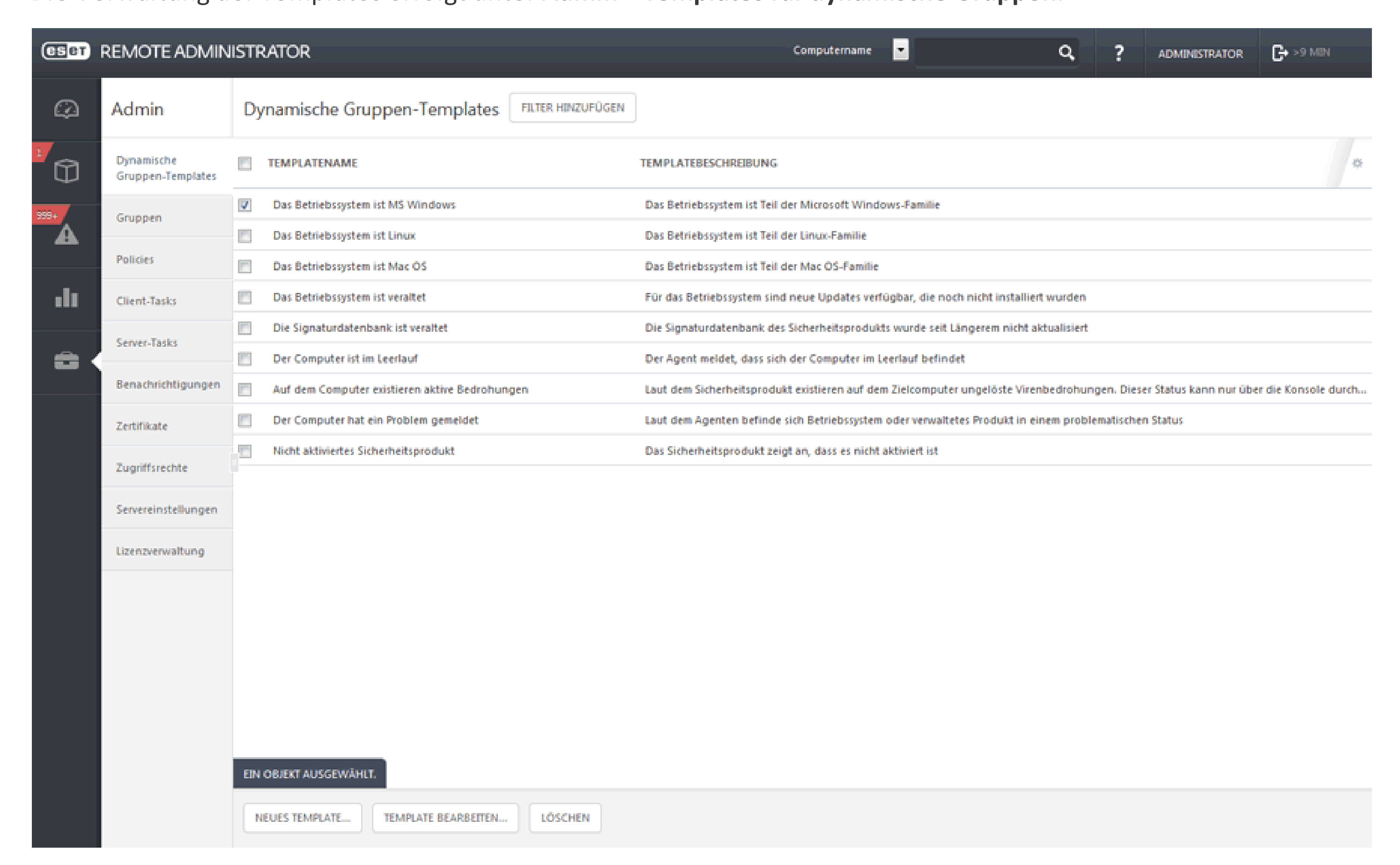
Zusammenfassung

Überprüfen Sie die konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**, um das neue Template zu erstellen. Das neue Template wird zur Liste der Templates hinzugefügt und kann später zum Erstellen einer neuen dynamischen Gruppe verwendet werden. Unter der Option **Ausdruck** können Sie Regeln/Bedingungen für die Gruppe konfigurieren (eine Beschreibung des Regel-Editors finden Sie hier). Jede auf diesem Template basierende dynamische Gruppe bewertet nun diese Regeln.

Klicken Sie zum Speichern Ihrer Änderungen auf **Fertig stellen**.

6.1.1.7.2 Verwalten von Templates für dynamische Gruppen

Die Verwaltung der Templates erfolgt unter **Admin** > **Templates für dynamische Gruppen**.



Sie können entweder ein neues Template erstellen oder eines der vorhandenen Templates bearbeiten. Zum Bearbeiten klicken Sie auf das gewünschte Template. Ein Assistent wird angezeigt. Alternativ können Sie ein Template durch Aktivieren des Kontrollkästchens neben dem Template auswählen und dann auf **Template bearbeiten** klicken.

Ausdruck

Wählen Sie einen logischen Operator im Menü **Operation** aus.

- **AND** – Alle festgelegten Bedingungen müssen erfüllt sein.
- **OR** – Mindestens eine Bedingung muss erfüllt sein.
- **NAND** – Mindestens eine Bedingung darf nicht erfüllt sein.
- **NOR** – Alle Bedingungen müssen falsch sein.

Wählen Sie beispielsweise **UND**. Dies bedeutet, dass der Computer alle Bedingungen erfüllen muss, um in der dynamischen Gruppe angezeigt zu werden, die dieses Template verwendet.

- Klicken Sie auf **+ Regel hinzufügen** und wählen Sie eine Bedingung aus. Nehmen wir an, Sie möchten Clients auswählen, die ein Notebook mit angeschlossenem Netzkabel verwenden. Wählen Sie **Hardware** > **Im Akkubetrieb** > **=(gleich)** > **Wird nicht entladen** aus.
- Klicken Sie auf **+ Regel hinzufügen**, um eine zweite Bedingung einzugeben (die Anzahl der Regeln ist unbegrenzt).Wählen Sie **Betriebssystemedition** > **OS-Typ** > **=(gleich)** > **Windows 8.1** (geben Sie diesen Wert in das leere Feld ein).

Wenn beide Bedingungen erfüllt sind, wird der Client in der dynamischen Gruppe angezeigt.

Zusammenfassung

Überprüfen Sie die konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**, um das neue Template zu erstellen. Das neue Template wird zur Liste der Templates hinzugefügt und kann später zum Erstellen einer neuen dynamischen Gruppe verwendet werden. Unter der Option **Ausdruck** können Sie Regeln/Bedingungen für die Gruppe konfigurieren (eine Beschreibung des Regel-Editors finden Sie hier). Jede auf diesem Template basierende dynamische Gruppe bewertet nun diese Regeln.

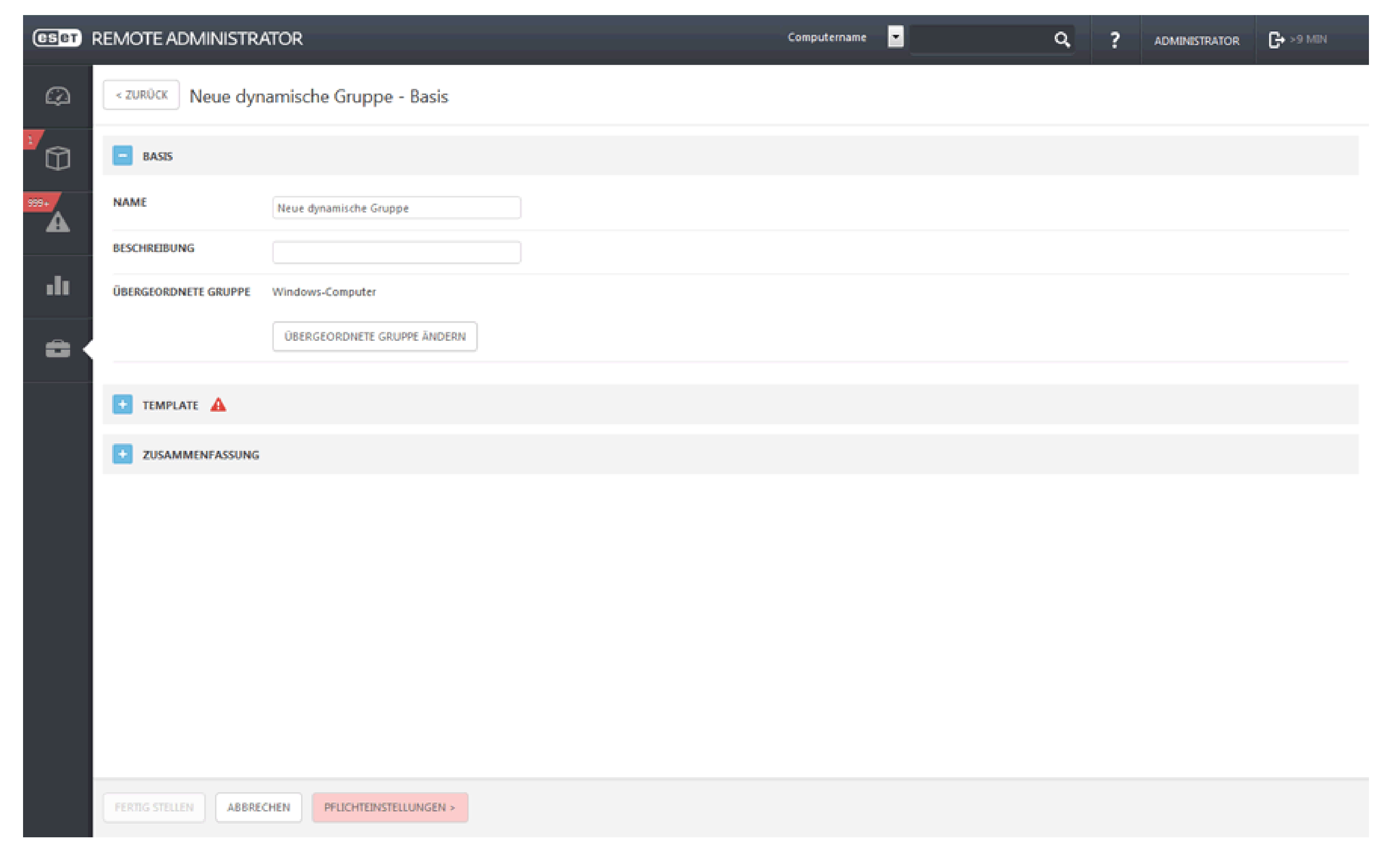
Klicken Sie zum Speichern Ihrer Änderungen auf **Fertig stellen**.

6.1.1.7.3 Assistent für dynamische Gruppen

Zum Erstellen einer dynamische Gruppe können Sie ein vorhandenes Template verwenden oder ein neues Template erstellen (das nach der Erstellung für diese dynamische Gruppe verwendet wird).

Basis

Geben Sie einen **Namen** und eine **Beschreibung** (optional) für die neue dynamische Gruppe ein. Standardmäßig ist die übergeordnete Gruppe die Gruppe, die Sie zu Beginn des Erstellungsvorgangs der neuen statischen Gruppe ausgewählt haben. Wenn Sie die übergeordnete Gruppe ändern möchten, klicken Sie auf **Übergeordnete Gruppe ändern** und wählen Sie eine aus der Baumstruktur aus. Die übergeordnete Gruppe der neuen dynamischen Gruppe kann eine dynamische oder eine statische Gruppe sein. Klicken Sie auf **Fertig stellen**, um die neue dynamische Gruppe zu erstellen.



Template

Sie können ein vorhandenes Template für dynamische Gruppen auswählen oder ein neues Template für dynamische Gruppen erstellen.

Zusammenfassung

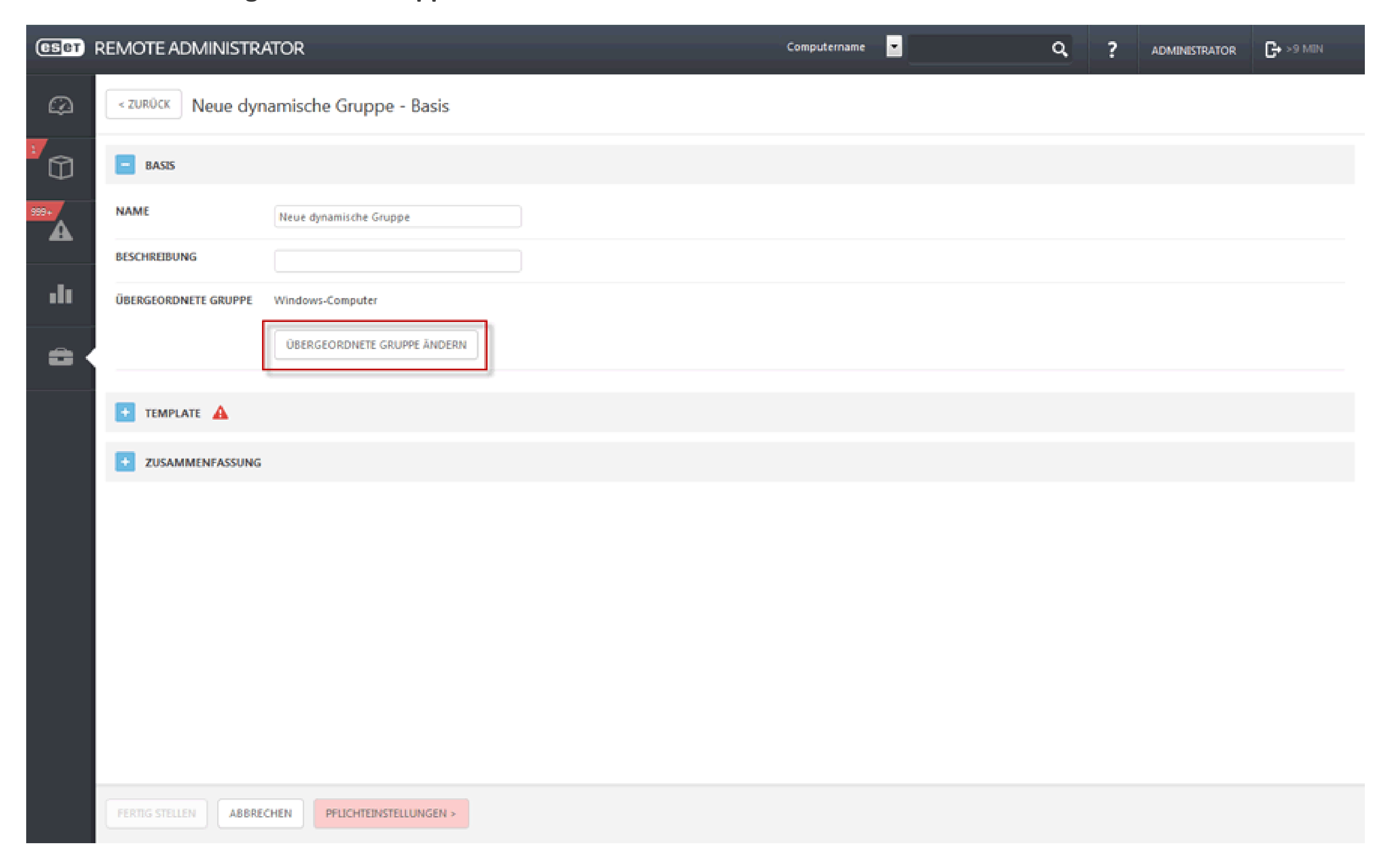
Überprüfen Sie die Konfiguration, um sicherzustellen, dass sie richtig ist. Nehmen Sie bei Bedarf Änderungen vor. Klicken Sie dann auf **Fertig stellen**.

6.1.1.7.4 Erstellen einer dynamischen Gruppe mit einem vorhandenen Template

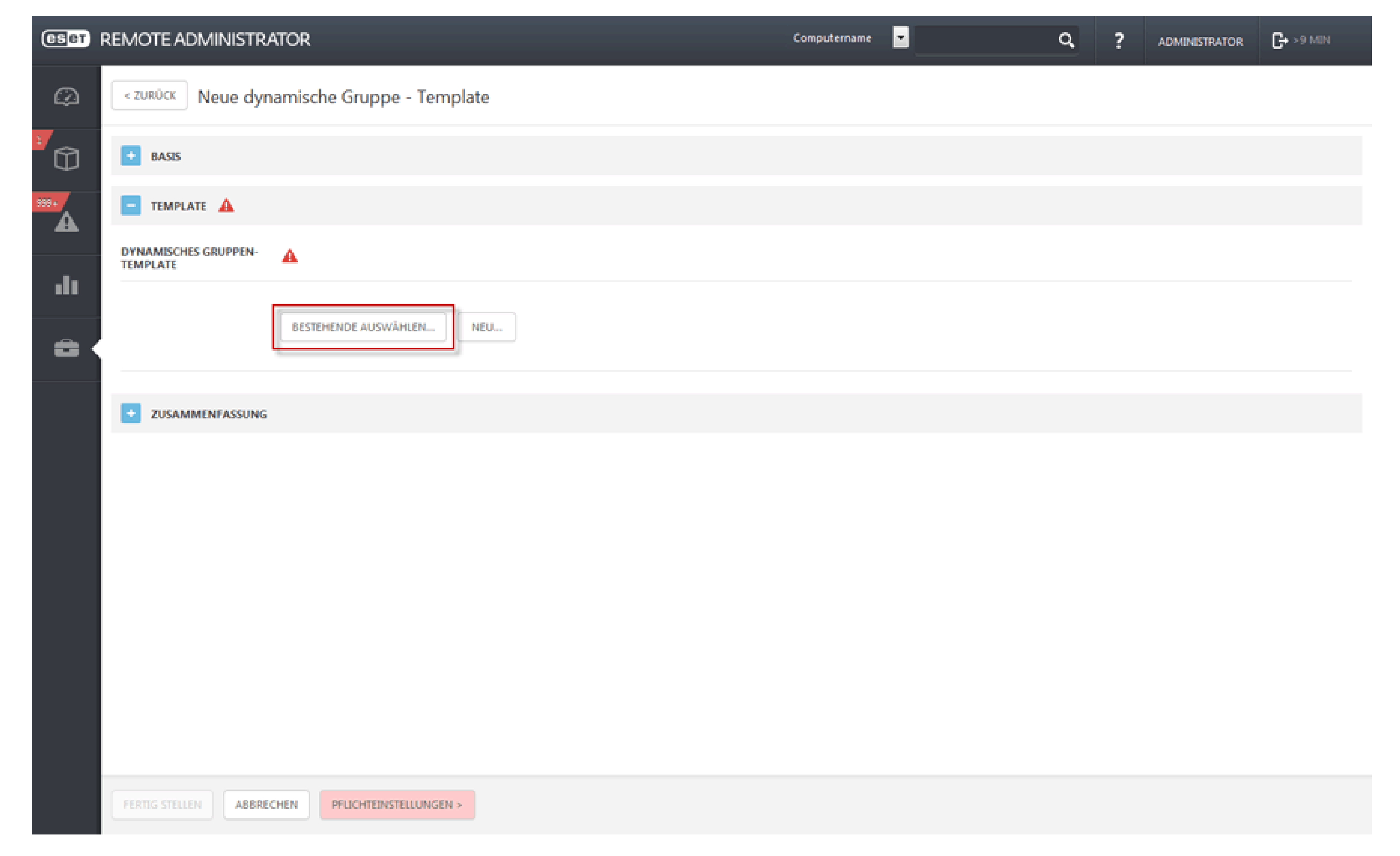
Um eine dynamische Gruppe unter Verwendung einer vorhandenen Vorlage zu erstellen, klicken Sie auf das Zahnradsymbol ⚙ neben dem Namen der dynamischen Gruppe und klicken Sie dann auf **Neue dynamische Gruppe**.

Alternativ ist die Funktion **Neue dynamische Gruppe ...** auch unter **Admin** > **Gruppen** verfügbar. Wählen Sie im Gruppenbereich eine Gruppe aus und klicken Sie unten auf **Gruppe**.

Der Assistent für dynamische Gruppen wird angezeigt. Geben Sie unter **Name** und (optional) unter **Beschreibung** die gewünschten Angaben für das neue Template ein. Sie können auch die übergeordnete Gruppe ändern. Klicken Sie hierzu auf **Übergeordnete Gruppe ändern**.



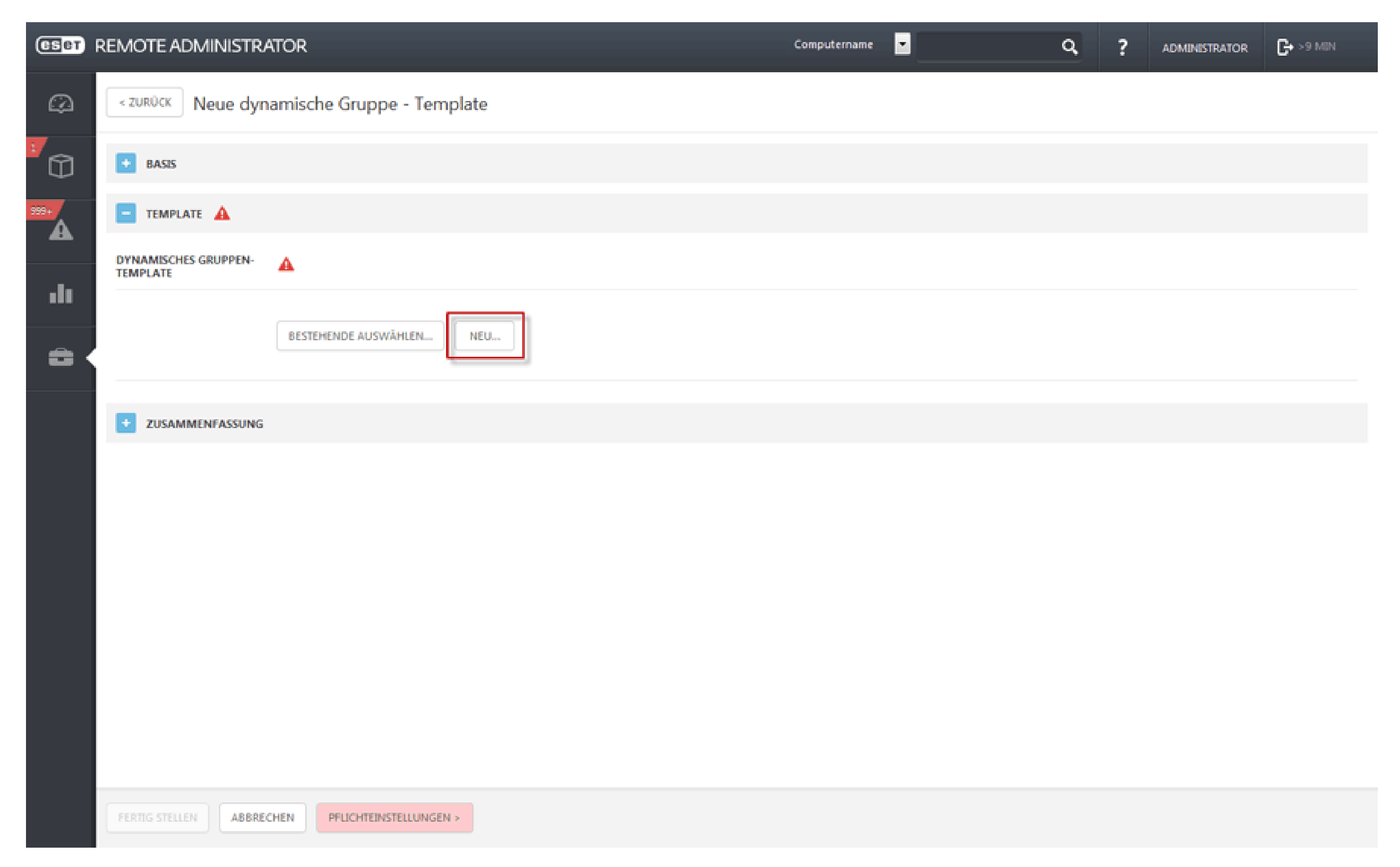
Wählen Sie ein **Template für dynamische Gruppe** aus den vordefinierten Templates oder aus bereits erstellten Templates aus. Klicken Sie auf **Bestehende auswählen ...** und wählen Sie in der Liste das gewünschte Template aus. Wenn Sie noch kein Template erstellt haben und keines der vordefinierten Templates in der Liste geeignet ist, klicken Sie auf „Neu ...“ und befolgen Sie die Anweisungen zum Erstellen eines neuen Template.



Der letzte Bildschirm enthält eine Zusammenfassung. Die neue Gruppe wird unter der übergeordneten statischen Gruppe angezeigt.

6.1.1.7.5 Erstellen einer dynamischen Gruppe mit einem neuen Template

Die Schritte sind die gleichen wie beim Erstellen einer dynamischen Gruppe mit einem vorhandenen Template, bis zum Schritt **Template für dynamische Gruppe**. Hier klicken Sie stattdessen Neues Template für dynamische Gruppen und füllen die Details für das neue Template aus.



Nach dem Fertigstellen wird automatisch das neue Template verwendet. Außerdem wird das Template in der Liste der Templates für dynamische Gruppen angezeigt und kann zum Erstellen weiterer dynamischer Gruppen verwendet werden.

6.1.1.7.6 Verwalten dynamischer Gruppen

Sie können dynamische Gruppen unter Verwendung eines vorhandenen Template erstellen oder ein neues Template erstellen, das dann für die dynamische Gruppe verwendet wird.

Nach der Erstellung können die Benutzer verschiedene Vorgänge für die dynamischen Gruppen ausführen. Dies umfasst folgende Aktionen:

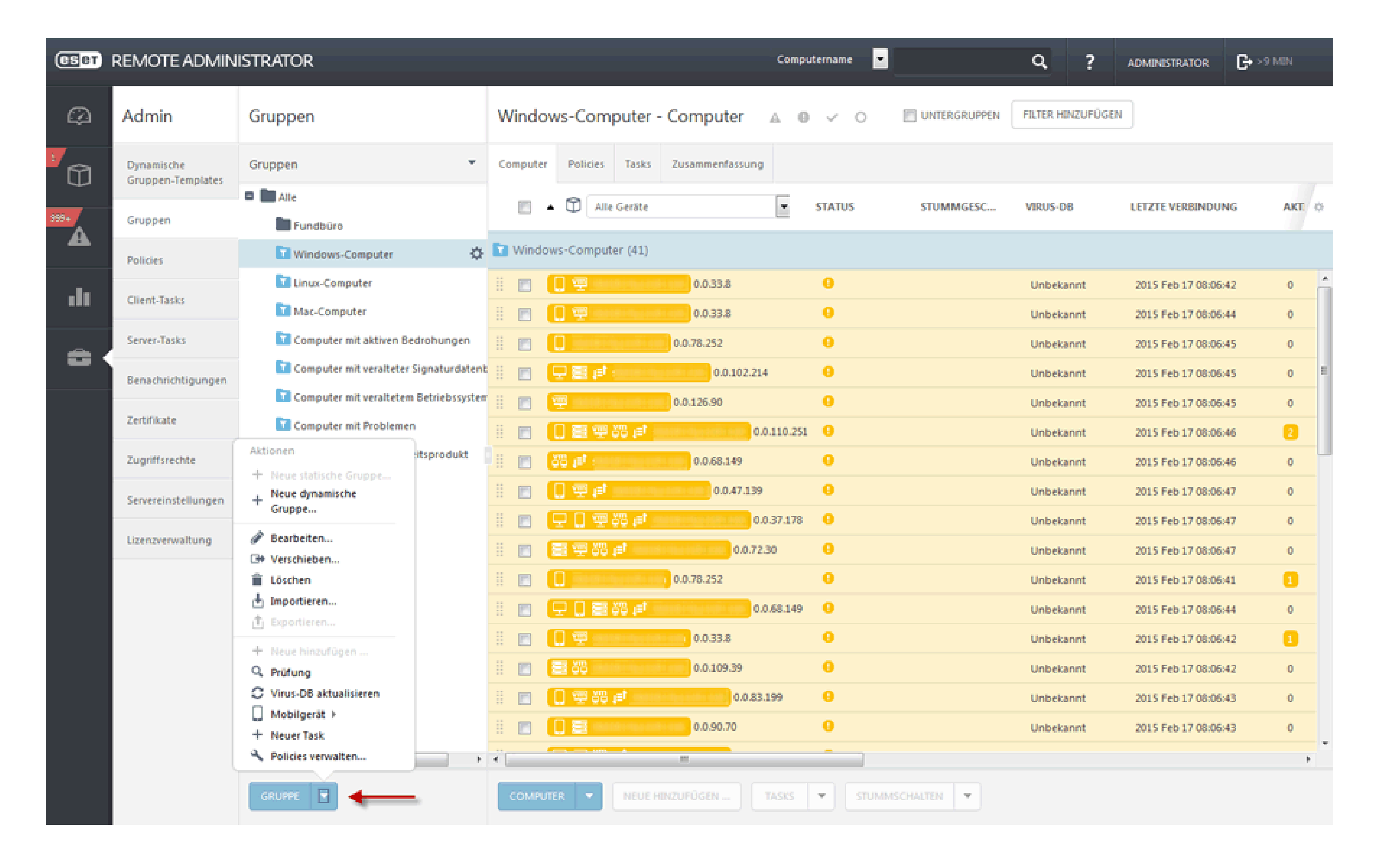
- Bearbeiten
- Verschieben
- Löschen
- Tasks ausführen
- Für Benachrichtigungen verwenden

Zum Zugriff auf diese Aktionen stehen die folgenden drei Möglichkeiten zur Verfügung:

1. **Computer** > **Gruppen** >

2. **Admin** > **Gruppen** >

3. Unter **Admin** > **Gruppen** die dynamischen Gruppen auswählen, die Sie verwalten möchten, und auf **Gruppe** klicken.



6.1.1.7.7 Verschieben einer dynamischen Gruppe

Klicken Sie auf das Zahnradsymbol ⚙ neben dem Gruppennamen und wählen Sie **Verschieben** aus. Ein Pop-up-Fenster mit der Baumstruktur der Gruppen wird angezeigt. Wählen Sie die (statische oder dynamische) Zielgruppe aus, in die Sie die ausgewählte Gruppe verschieben möchten. Die Zielgruppe wird eine übergeordnete Gruppe. Sie können eine Gruppe auch durch Ziehen der Gruppe und Ablegen in der gewünschten Zielgruppe verschieben.

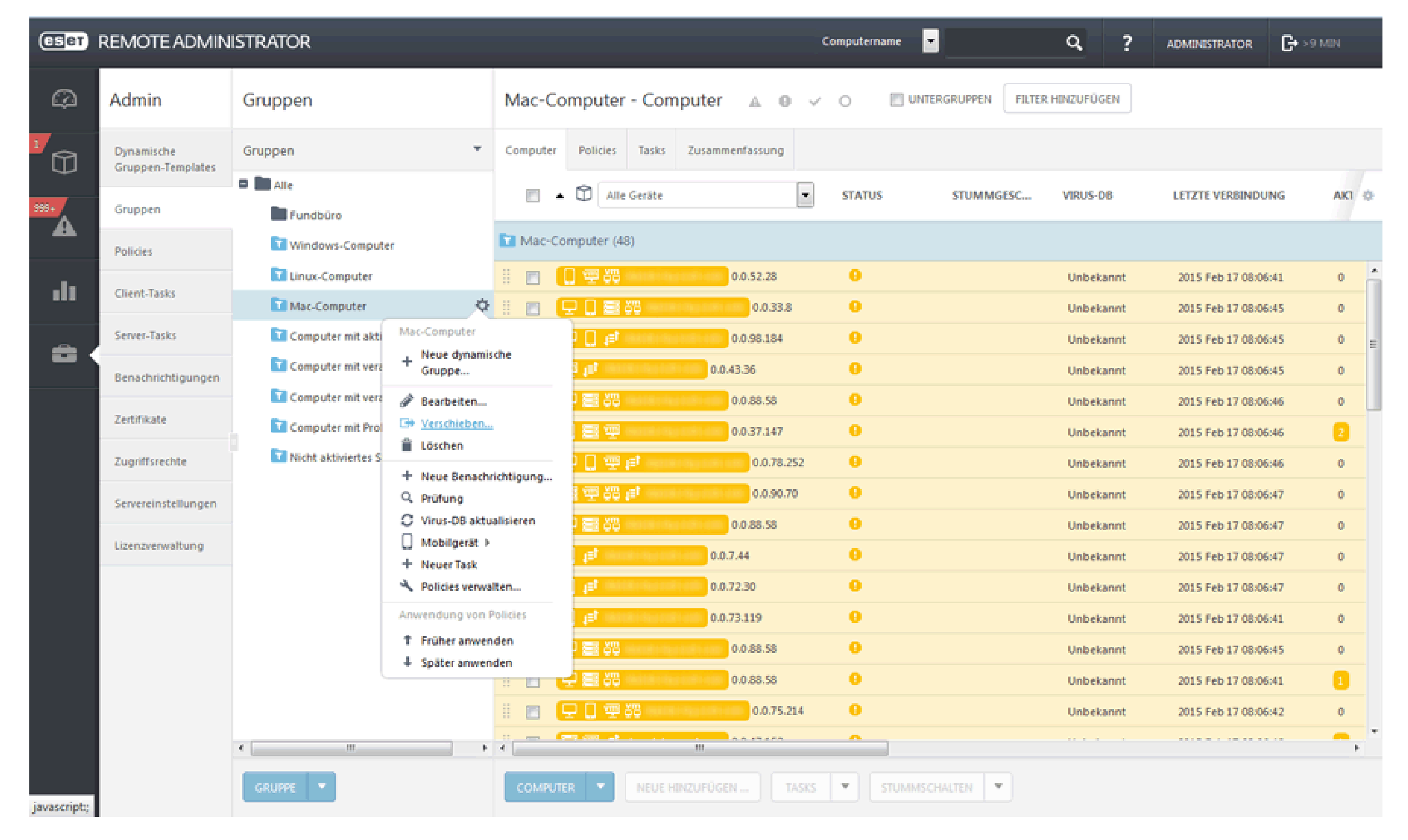
Einige Ausnahmen bei der Gruppenorganisation müssen beachtet werden. **Eine statische Gruppe kann nicht in eine dynamische Gruppe** verschoben werden. Außerdem können keine vordefinierten statischen Gruppen (zum Beispiel die Gruppe „Fundbüro“) in eine andere Gruppe verschoben werden. Andere Gruppen können frei verschoben werden. Eine dynamische Gruppe kann Mitglied einer beliebigen anderen Gruppe sein, auch einer statischen Gruppe.

Zum Verschieben von Gruppen stehen folgende Methoden zur Verfügung:

Ziehen und Ablegen - Klicken Sie auf die zu verschiebende Gruppe und halten Sie die Maustaste gedrückt. Bewegen Sie den Mauszeiger zur neuen übergeordneten Gruppe Ihrer Wahl und lassen Sie die Maustaste los.

⚙ > **Bearbeiten** > **Übergeordnete Gruppe ändern**.

⚙ > **Verschieben** > Auswahl einer neuen übergeordneten Gruppe aus der Liste und Klicken auf **OK**.



HINWEIS: Eine dynamische Gruppe filtert Computer (basierend auf dem Template) an ihrer neuen Position ohne jeglichen Bezug zur früheren Position der Gruppe.

6.1.1.7.8 Zuweisen einer Policy zu einer dynamischen Gruppe

In Bezug auf die Zuweisung von Policies werden statische und dynamische Gruppen gleich behandelt. Anweisungen zum Zuweisen einer Policy zu einer Gruppe finden Sie hier.

6.1.1.7.9 Zuweisen eines Task zu einer dynamischen Gruppe

In Bezug auf die Zuweisung von Tasks werden statische und dynamische Gruppen gleich behandelt. Anweisungen zum Zuweisen eines Tasks zu einer Gruppe finden Sie hier.

6.1.1.7.10 Automatisieren von ESET Remote Administrator

1. Erstellen Sie eine dynamische Gruppe, zum Beispiel: „Infizierte Computer“
2. Erstellen Sie einen Task für einen Tiefen-Scan und weisen Sie ihn der dynamischen Gruppe „Infizierte Computer“ zu (Task wird ausgelöst, wenn ein Client Mitglied der dynamischen Gruppe wird).
3. Erstellen Sie eine bestimmte Policy (in diesem Fall eine „Isolierungs-Policy“): Wenn ein ESET-Sicherheitsprodukt installiert wird, eine Firewall-Regel erstellen, die den gesamten Verkehr außer der Verbindung zu ESET Remote Administrator blockiert.
4. Erstellen Sie ein Benachrichtigungs-Template für infizierte Computer. Sie können verschiedene Bedingungen festlegen. Eine Benachrichtigung wird ausgelöst, um Sie vor einer sich verbreitenden Bedrohung zu warnen.

- Mit der gleichen Methode können Sie auch Produkt- und Betriebssystem-Updates, Scans, automatische Aktivierungen neu hinzugefügter Produkte mit einer vorausgewählten Lizenz und andere Tasks automatisieren.

6.1.1.7.11 Wann wird ein Computer Mitglied einer dynamischen Gruppe?

Ein Computer muss bestimmte Bedingungen erfüllen, um Mitglied einer dynamischen Gruppe zu werden. Diese Bedingungen werden in einem Template für die dynamische Gruppe definiert. Jedes Template enthält eine oder mehrere Regeln (=Bedingungen). Sie können diese Regeln beim Erstellen eines neuen Template festlegen.

Bestimmte Informationen zum aktuellen Status eines Clientcomputers werden im Agenten gespeichert. Der Status des Computers wird dann vom Agenten auf Grundlage der Regeln für das Template bewertet.

ERA-Benutzer sind unter Umständen nur an bestimmten Status interessiert. In diesem Fall kann der Benutzer den gewünschten Status durch Festlegen von Werten definieren. Dies vordefinierte Satz wird als dynamische Gruppe bezeichnet.

Sobald ein beliebiger Computer den Status mit diesen bestimmten Werten erfüllt, wird er der Gruppe zugewiesen.

Dynamische Gruppen können als Filter in Bezug auf den Computerstatus betrachtet werden. Ein Computer kann mehrere Filter erfüllen und daher mehr als einer dynamischen Gruppe zugeordnet werden. Darin unterscheiden sich dynamische Gruppen von statischen Gruppen, da ein Computer immer nur in einer statischen Gruppe vorhanden sein kann.

6.1.1.7.12 Bewertung der Template-Regeln

Die Bewertung der Template-Regeln wird vom Agenten vorgenommen, nicht vom ERA-Server. Lediglich das Ergebnis wird an den ERA-Server gesendet. Der Bewertungsvorgang wird gemäß den Regeln ausgeführt, die für ein Template konfiguriert sind. Der Bewertungsprozess wird nachfolgend mit einigen Beispielen beschrieben.

Der Status setzt sich aus verschiedenen Informationen zusammen. Bestimmte Quellen stellen mehrere eindimensionale Status je Computer zur Verfügung (zum Beispiel Betriebssystem und Größe des Arbeitsspeichers), andere stellen mehrdimensionale Statusinformationen bereit (wie IP-Adresse oder installierte Anwendung).

Nachfolgend finden Sie eine visuelle Darstellung eines Clientstatus:

Netzwerkadapter.IP-Adresse	Netzwerkadapter.MAC-Adresse	Betriebssystemname	Betriebssystemversion	HW-Arbeitsspeichergröße in MB	Installierte Anwendung
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Der Status setzt sich aus Informationsgruppen zusammen. Eine Datengruppe enthält in Zeilen angeordnete, kohärente Informationen. Die Anzahl der Zeilen je Gruppe kann variieren.

Die Bedingungen werden nach Gruppe und nach Zeile bewertet. Wenn für die Spalten einer Gruppe mehrere Bedingungen vorliegen, werden nur Werte einer gleichen Zeile berücksichtigt.

Beispiel 1:

In diesem Beispiel gilt folgende Bedingung:

```
Netzwerkadapter.IP-Adresse = 10.1.1.11 AND Netzwerkadapter.MAC-Adresse = 4A-64-3F-10-FC-75
```

Kein Computer stimmt mit dieser Regel überein, da keine Zeile beide Bedingungen erfüllt.

Netzwerkadapter - IP-Adresse	Netzwerkadapter - MAC-Adresse	Betriebssystemname	Betriebssystemversion	HW-Arbeitsspeichergröße in MB	Installierte Software
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Beispiel 2:

In diesem Beispiel gilt folgende Bedingung:

```
Netzwerkadapter.IP-Adresse = 192.168.1.2 AND Netzwerkadapter.MAC-Adresse = 4A-64-3F-10-FC-75
```

Diesmal erfüllen Zellen in einer einzigen Zeile beide Bedingungen. Daher wird die Regel als WAHR bewertet. Ein Computer wird ausgewählt.

Netzwerkadapter - IP-Adresse	Netzwerkadapter - MAC-Adresse	Betriebssystemname	Betriebssystemversion	HW-Arbeitsspeichergröße in MB	Installierte Software
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite

					Weather Forecast

Beispiel 3:

Bei Bedingungen mit dem Operator „OR“ (mindestens eine Bedingung muss WAHR sein) wie

```
Netzwerkadapter.IP-Adresse = 10.1.1.11 OR Netzwerkadapter.MAC-Adresse = 4A-64-3F-10-FC-75
```

ist die Regel für zwei Zeilen WAHR, da nur eine der beiden Bedingungen erfüllt werden muss. Ein Computer wird ausgewählt.

Netzwerkadapter - IP-Adresse	Netzwerkadapter - MAC-Adresse	Betriebssystemname	Betriebssystemversion	HW-Arbeitsspeichergröße in MB	Installierte Software
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

6.1.1.7.13 Regel-Editor

Bedingungen

Für das Festlegen von Bedingungen für ein Template einer dynamischen Gruppe stehen je nach Bedingung verschiedene Operatoren zur Verfügung.

Es gibt 3 Arten von Listen:

- Listen mit numerischen Operatoren enthalten Operatoren zum Vergleich von Zahlenwerten.
- Listen mit Zeichenfolgen-Operatoren enthalten Operatoren zum Vergleich von Zeichenfolgen.
- Listen mit booleschen Operatoren enthalten nur die Operatoren „wahr“ („= (gleich)“) und „falsch“ („≠ (ungleich)“).

Arten von Operatoren

Die Liste enthält 6 Werte:

- „= (ist gleich)“
- „≠ (ungleich)“
- „> (größer als)“
- „≥ (größer gleich)“
- „< (kleiner als)“
- „≤ (kleiner gleich)“

Zeichenfolgenoperatoren

Die Liste enthält 9 Werte:

- „= (ist gleich)“ - Nur den genauen und vollständigen gesuchten Wert festlegen.
- „≠ (ungleich)“ - Nur den genauen und vollständigen Wert festlegen, der in der Suche ignoriert werden soll.
- „hat Teilzeichenfolge“ - Zeichenfolge festlegen, die im Ausdruck enthalten sein soll.
- „hat Präfix“ - Die genauen ersten Zeichen der gesuchten Zeichenfolge festlegen, z. B. für die gesuchte Zeichenfolge „Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319“ den Präfix „Micros“ oder „Micr“ oder „Microsof“.
- „hat Postfix“ - Die genauen letzten Zeichen der gesuchten Zeichenfolge festlegen, z. B. für die gesuchte Zeichenfolge „Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319“ den Postfix „319“ oder „0.30319“.
- „RegEx“ - Perl-Syntax
- „in“ - Einen genauen Ausdruck festlegen, zum Beispiel für „Microsoft Windows“ genau „Microsoft Windows“.
- „hat Maske“ und „in (Zeichenfolgenmaske)“ haben 2 Arten von Platzhalterzeichen:
- * - Platzhalter für eine beliebige Anzahl Ziffern oder Zeichen (0 oder mehr)
- ? - genau 1 übereinstimmendes Zeichen

Beispiele

- „a*“ kann für „a“, „aa“, „ax“, „abcde“ stehen.
- „a?“ kann für „aa“, „ab“, ,„ac“ stehen, nicht jedoch für „a“ oder „aaa“.
- „a??“ kann für „aaa“, „aab“, ,„axy“ stehen, nicht jedoch für „a“, „aa“ oder „aaaa“.
- „a?*“ kann für „aa“, „ax“, „abcde“ stehen, nicht jedoch für „a“.
- „*a*“ kann für „a“, „xa“, „ax“, „xax“, „dynamisch“, „abba“ stehen.
- „?*“ passt für alle Zeichenfolgen außer „“.

Boolesche Operatoren

Die Liste enthält 2 Werte. Die Werte sind immer mit der zweiten Bedingung verknüpft.

- „= (gleich)“ - Die nächste Bedingung ist wahr.
- „≠ (ungleich)“ - Die nächste Bedingung ist falsch.

- Die mathematischen Basisoperationen (z. B. größer als) sind selbsterklärend. Für die sonstigen Operationen finden Sie hier eine kurze Beschreibung:

hat Teilzeichenfolge“-Operator. Gilt, wenn der Operand eine Teilzeichenfolge des Symbolwerts ist.
„hat Präfix“-Operator. Gilt, wenn der Symbolwert mit dem Wert des Operanden beginnt. Z. B. „xyz“ hat das Präfix „xy“.
„hat Postfix“-Operator. Gilt, wenn der Symbolwert mit dem Wert des Operanden endet. Z. B. „xyz“ hat das Postfix „yz“.
„hat Maske“-Operator. Ermöglicht die Verwendung von Platzhaltern für Zeichenfolgenvergleiche. Z. B. „*z“ gilt für „xyz“
„regex“-Operator. Gilt, wenn das Symbol mit dem regulären Ausdruck im Operanden übereinstimmt. Für reguläre Ausdrücke gilt die Perl-Syntax.
„in“-Operator. Der Operand enthält eine Liste von Werten. Gilt, wenn der Symbolwert mit mindestens einem der Operandenwerte übereinstimmt. Z. B. „xyz“ in („abc“, „def“, „xyz“).
„in (String-Maske)“-Operator. Der Operand enthält eine Liste von Werten, die Platzhalter enthalten können. Gilt, wenn der Symbolwert mit mindestens einem der Operandenwerte übereinstimmt. Z. B. „xyz“ in („a*“, „*f“, „*z“).
„hat keinen Wert“-Operator. Gilt, wenn das Symbol keinen Wert hat. Der zweite Operand wird ignoriert.
„hat Wert“-Operator. Gilt, wenn das Symbol einen Wert hat. Der zweite Operand wird ignoriert.

6.1.2 Policies

Policies werden dazu verwendet, bestimmte Konfigurationen auf ESET-Sicherheitsprodukte zu übertragen, die auf Clientcomputern ausgeführt werden. So müssen Sie die ESET-Produkte der Clients nicht einzeln manuell konfigurieren. **Eine Policy kann direkt auf einzelne** Computer oder auf (statische oder dynamische) Gruppen angewendet werden. Sie können einem Computer oder einer Gruppe auch mehrere Policies zuweisen. Dies ist ein wesentlicher Unterschied zu ESET Remote Administrator 5 und früheren Versionen, wo einem Produkt oder eine Komponente nur eine einzige Policy zugewiesen werden konnte.

Anwendung von Policies

Policies werden in der Anordnungsreihenfolge der statischen Gruppe angewendet. Dies gilt nicht für dynamische Gruppen. Hier werden zuerst die untergeordneten dynamischen Gruppen durchlaufen. So können Sie Policies mit größeren Auswirkungen oben in der Gruppenstruktur definieren und detailliertere Policies auf Untergruppen anwenden. Bei richtig konfigurierten Policies mit Markierungen kann ein ERA-Benutzer mit Zugriff auf Gruppen weiter oben in der Baumstruktur die Policies niedrigerer Gruppen unterdrücken. Der Algorithmus wird unter Anwenden von Policies auf einen Client ausführlich beschrieben.

Zusammenführen von Policies

Die auf einen Client angewendete Policy ist üblicherweise das Ergebnis mehrerer Policies, die in einer endgültigen Policy zusammengeführt sind.

HINWEIS: Es empfiehlt sich, Gruppen weiter oben in der Baumstruktur allgemeine Policies zuzuweisen (z. B. allgemeine Einstellungen wie der Update-Server). Detailliertere Policies (zum Beispiel Einstellungen für die Medienkontrolle) sollten weiter unten in der Gruppenbaumstruktur angewendet werden. Die niedriger gelegene Policy unterdrückt beim Zusammenführen üblicherweise die Einstellungen der höheren Policies (sofern nicht mit Policy-Markierungen anderweitig definiert).

HINWEIS: Wenn Sie eine vorhandene Policy später entfernen, wird die Konfiguration der Clientcomputer nach dem Entfernen der Policy nicht automatisch auf die ursprünglichen Einstellungen zurückgesetzt. Die Konfiguration bleibt so erhalten, wie sie gemäß der letzten auf die Clients angewendeten Policy festgelegt wurde. Dies gilt auch, wenn ein Computer Mitglied einer Dynamischen Gruppe wird, auf die eine bestimmte Policy angewendet wird, die die Computereinstellungen ändert. Diese Einstellungen werden beibehalten, auch wenn der Computer aus der dynamischen Gruppe entfernt wird. Es empfiehlt sich daher, eine Policy mit Standardeinstellungen zu erstellen und diese Policy einer Stammgruppe (**Alle**) zuzuweisen. So können die Einstellungen in einem solchen Fall auf die Standardeinestellungen zurückgesetzt werden. Wenn ein Computer aus einer dynamischen Gruppe entfernt wird, die die Computereinstellungen geändert hat, werden die Einstellungen so wieder auf die Standardwerte zurückgesetzt.

6.1.2.1 Assistent für Policies

Mit Policies können Sie Ihr ESET-Produkt auf die gleiche Weise konfigurieren, wie über das Fenster für die erweiterten Einstellungen in der Benutzeroberfläche des Produkts. Anders als Policies in Active Directory können ERA-Policies keine Skripte oder Befehlsfolgen enthalten.

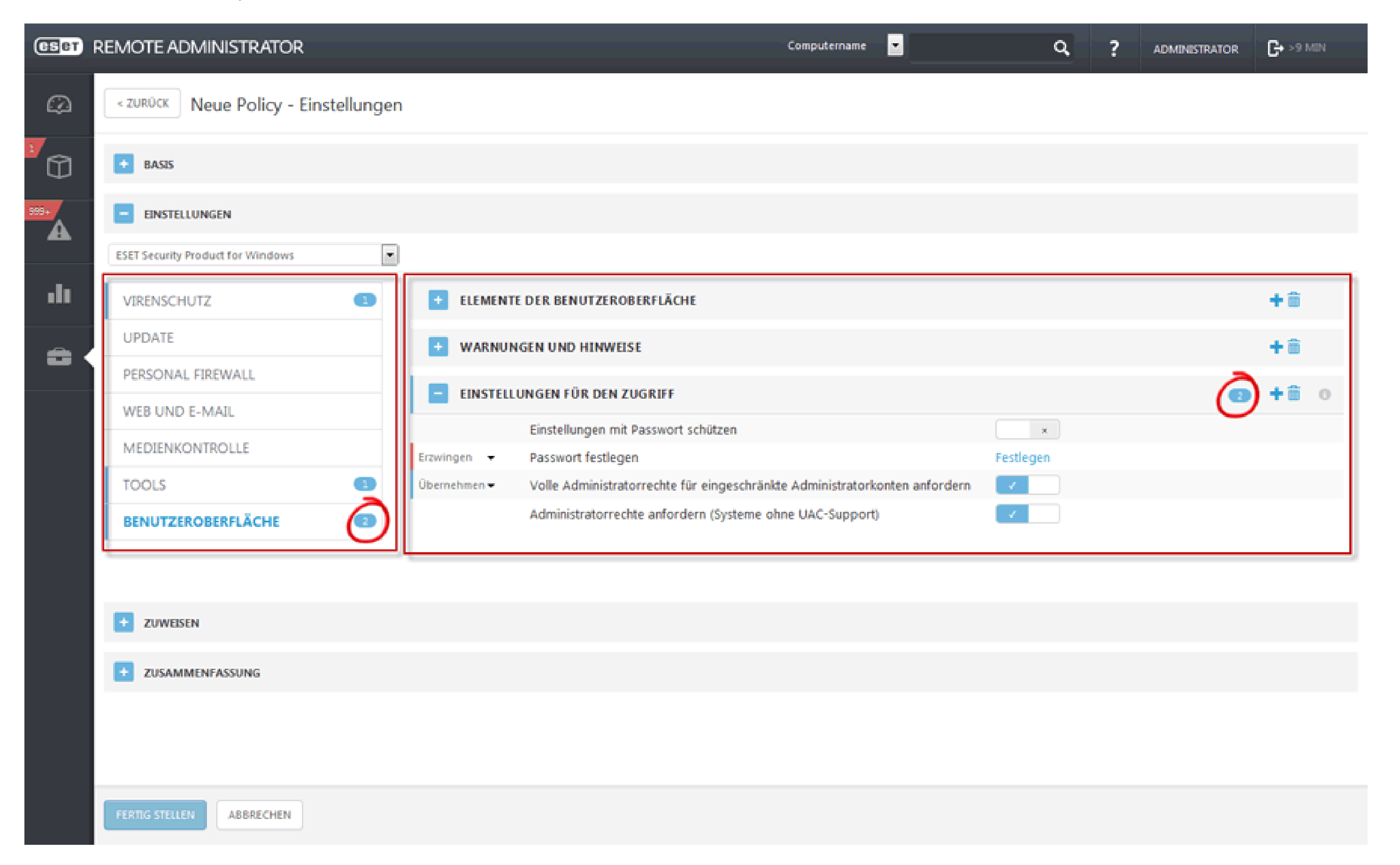
Policies werden über die Registerkarte **Admin** > **Policies** erstellt und verwaltet. Klicken Sie unten auf **Policies** und wählen Sie Neu aus dem Kontextmenü aus.

Basis

Geben Sie einen **Namen** für die neue Policy ein. Das Feld **Beschreibung** ist optional.

Einstellungen

Wählen Sie im Dropdown-Menü ein Produkt aus.



Wählen Sie links in der Baumstruktur eine Kategorie aus. Bearbeiten Sie die Einstellungen auf der rechten Seite nach Bedarf. Jede Einstellung ist eine Regel, für die Sie eine Markierung festlegen können. Zur Vereinfachung der Navigation wird die Gesamtzahl aller Regeln berechnet. Die Anzahl aller in einem bestimmten Bereich definierten Regeln wird automatisch angezeigt. Außerdem wird neben den Kategorienamen links in der Baumstruktur eine weitere Zahl angezeigt. Dies ist die Summe der Regeln in den einzelnen Bereichen. Hier können Sie auf einen Blick sehen, wo und wie viele Einstellungen/Regeln definiert sind.

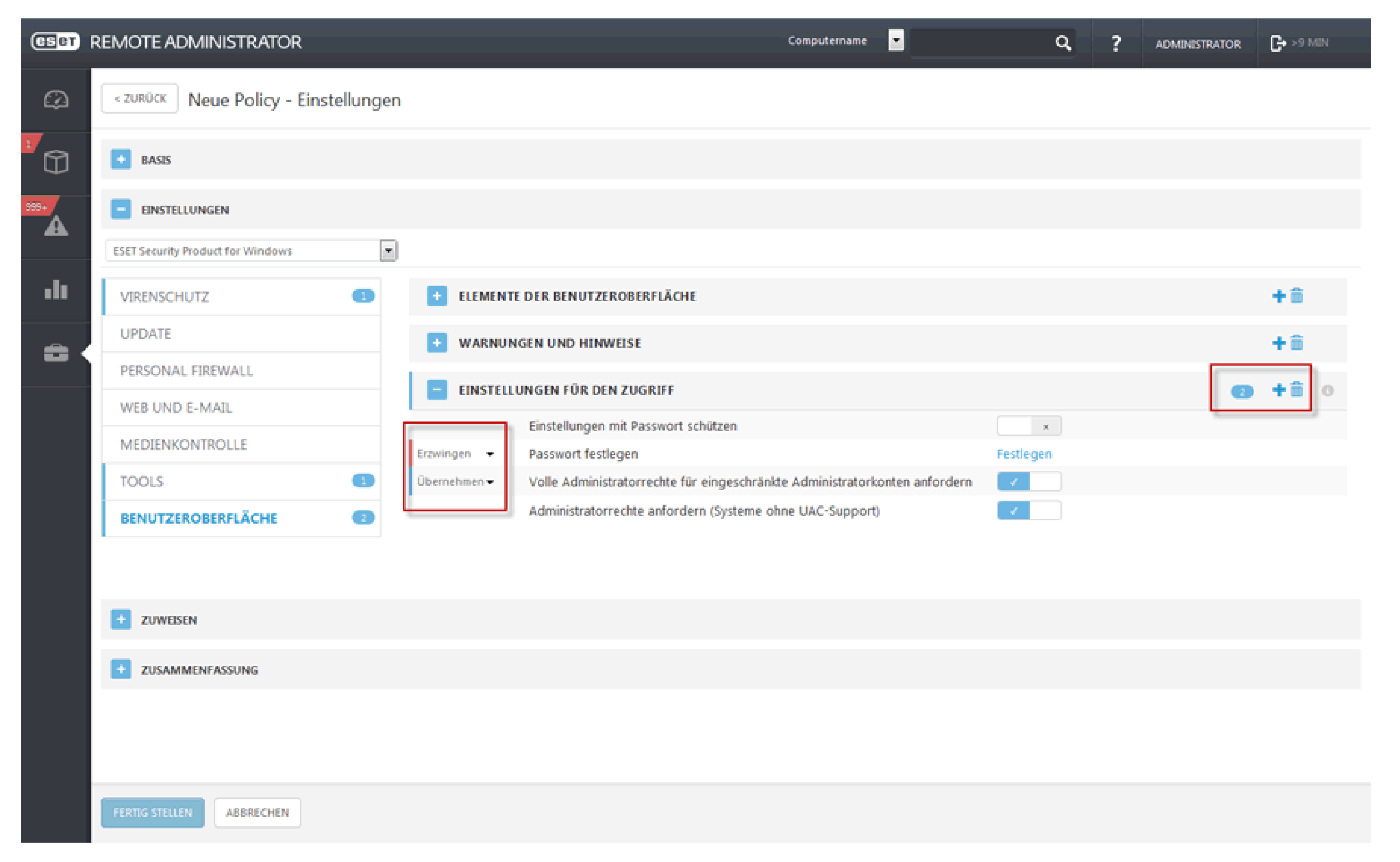
Mit den folgenden Empfehlungen können Sie die Bearbeitung von Policies vereinfachen:

- + verwenden, um die **Übernehmen**-Markierung für alle Elemente im aktuellen Bereich zu setzen
- Regeln mit dem **Papierkorb**-Symbol löschen

6.1.2.2 Markierungen

Sie können für jede Einstellung in einer Policy eine Markierung festlegen. Markierungen legen fest, wie die Einstellung von der Richtlinie behandelt wird:

- Anwenden - Einstellungen mit dieser Markierung werden an den Client gesendet. Durch das Zusammenführen von Policies kann die Einstellung jedoch durch eine spätere Policy überschrieben werden. Wenn eine Policy auf einen Clientcomputer angewendet wird und eine bestimmte Einstellung diese Markierung hat, wird die Einstellung unabhängig von der lokalen Konfiguration auf dem Client geändert. Die Einstellung ist jedoch nicht erzwungen und kann daher von anderen Policies geändert werden.
- Erzwingen - Einstellungen mit dieser Markierung sind prioritär und können nicht durch eine spätere Policy überschrieben werden (auch wenn diese ebenfalls die Markierung „Erzwingen“ hat). Dies gewährleistet, dass die Einstellung beim Zusammenführen nicht durch spätere Policies geändert wird.



Wählen Sie links in der Baumstruktur eine Kategorie aus. Bearbeiten Sie die Einstellungen auf der rechten Seite nach Bedarf. Jede Einstellung ist eine Regel, für die Sie eine Markierung festlegen können. Zur Vereinfachung der Navigation wird die Gesamtzahl aller Regeln berechnet. Die Anzahl aller in einem bestimmten Bereich definierten Regeln wird automatisch angezeigt. Außerdem wird neben den Kategorienamen links in der Baumstruktur eine weitere Zahl angezeigt. Dies ist die Summe der Regeln in den einzelnen Bereichen. Hier können Sie auf einen Blick sehen, wo und wie viele Einstellungen/Regeln definiert sind.

Mit den folgenden Empfehlungen können Sie die Bearbeitung von Policies vereinfachen:

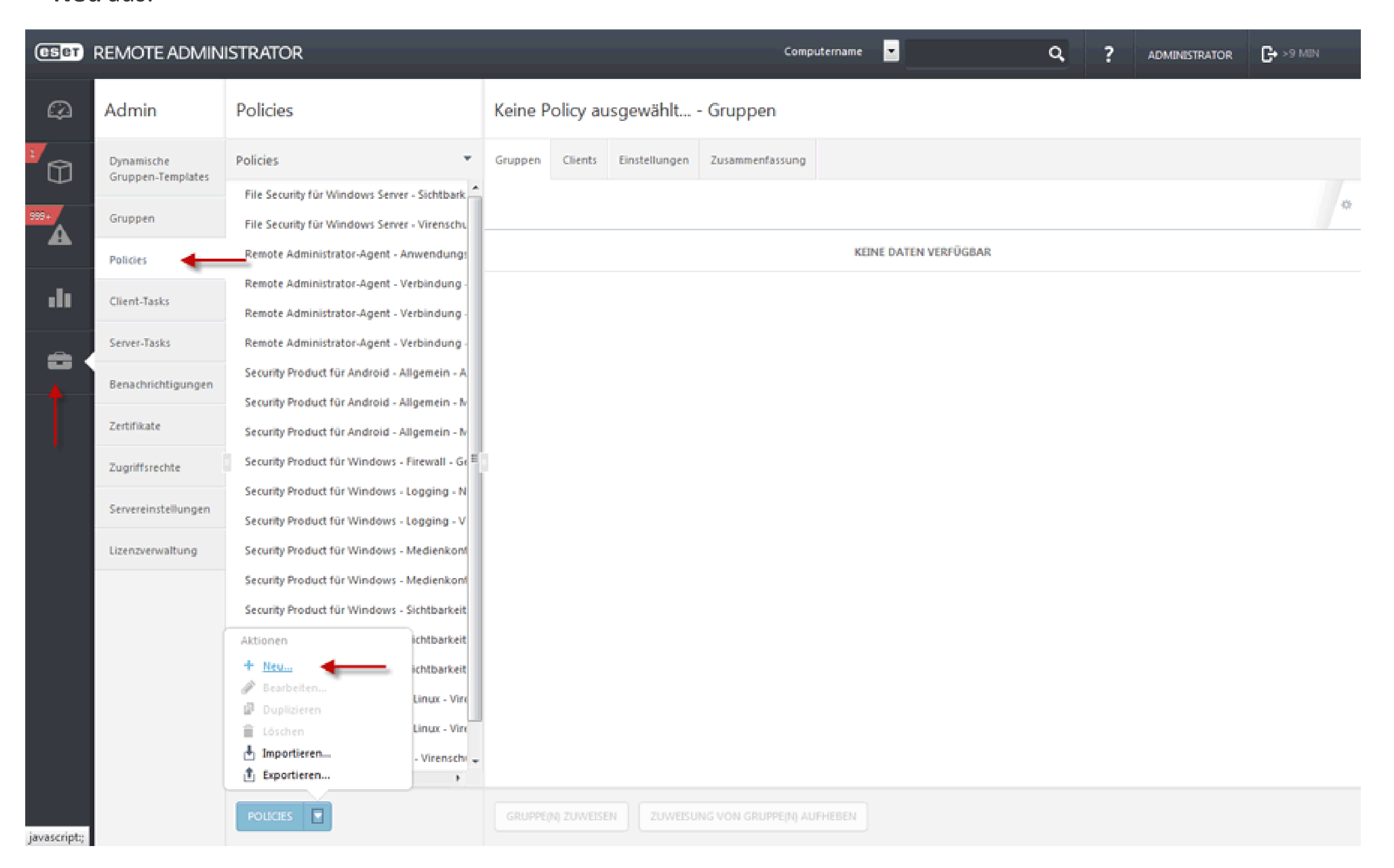
- + verwenden, um die **Übernehmen**-Markierung für alle Elemente im aktuellen Bereich zu setzen
- Regeln mit dem **Papierkorb**-Symbol löschen

6.1.2.3 Verwalten von Policies

In diesem Beispiel erstellen wir eine neue Policy für das Verbindungsintervall des ERA-Agenten. Testen Sie diesen Vorgang vor der massenhaften Bereitstellung unbedingt in Ihrer Umgebung.

1. Erstellen Sie eine Neue statische Gruppe.

2. Klicken Sie zum Erstellen einer neuen Policy auf **Admin** > **Policies**. Klicken Sie unten auf **Policies** und wählen Sie **Neu** aus.

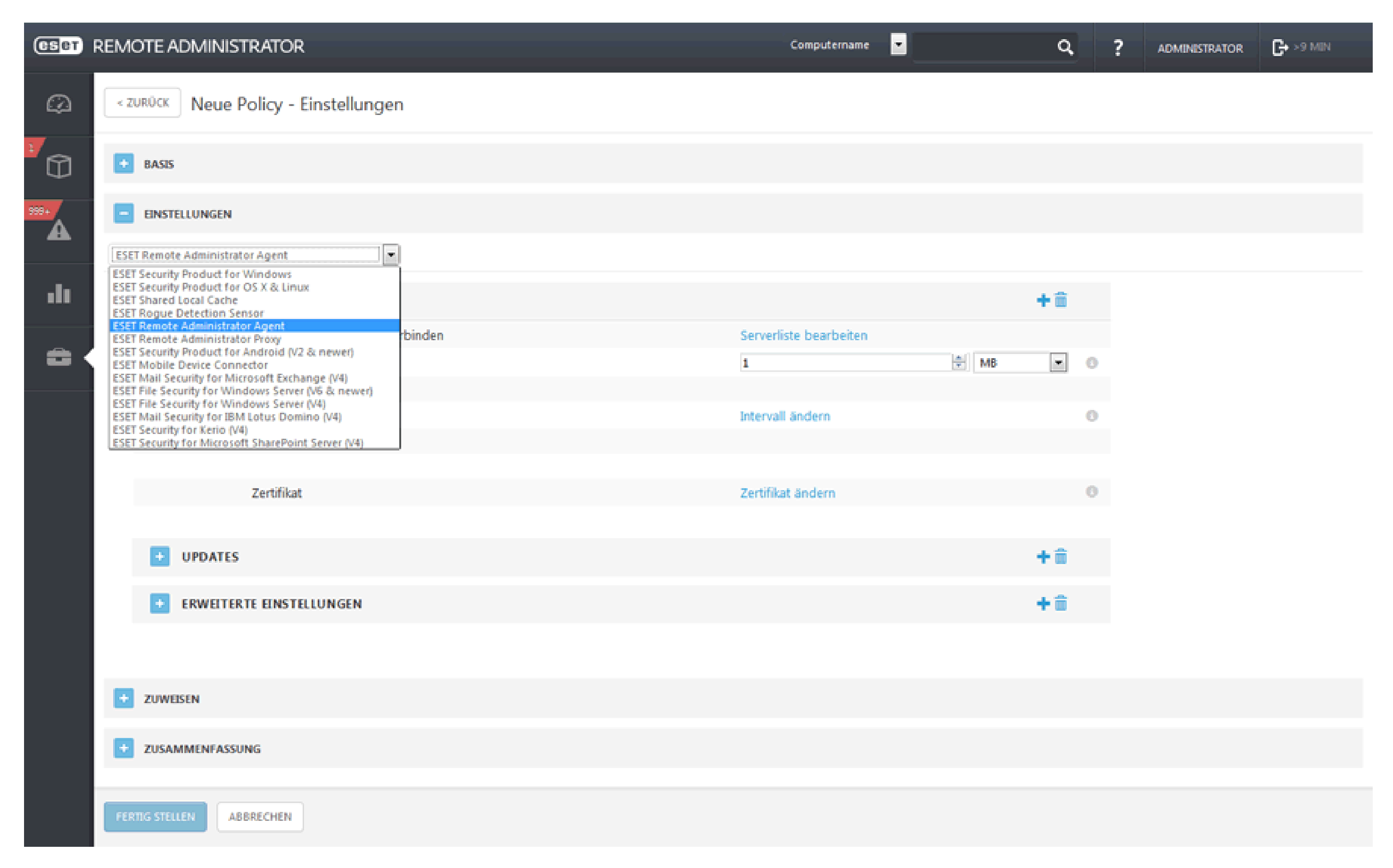


Basis

Geben Sie einen **Namen** für die neue Policy ein (zum Beispiel „Verbindungsintervall für Agent“). Die Eingabe in das Feld **Beschreibung** ist optional.

Einstellungen

Wählen Sie im Dropdownmenü **Produkt** den Eintrag **ESET Remote Administrator-Agent** aus.



Verbindung

Wählen Sie links in der Baumstruktur eine Kategorie aus. Bearbeiten Sie die Einstellungen auf der rechten Seite nach Bedarf. Jede Einstellung ist eine Regel, für die Sie eine Markierung festlegen können. Zur Vereinfachung der Navigation wird die Gesamtzahl aller Regeln berechnet. Die Anzahl aller in einem bestimmten Bereich definierten Regeln wird automatisch angezeigt. Außerdem wird neben den Kategorienamen links in der Baumstruktur eine weitere Zahl angezeigt. Dies ist die Summe der Regeln in den einzelnen Bereichen. Hier können Sie auf einen Blick sehen, wo und wie viele Einstellungen/Regeln definiert sind.

Mit den folgenden Empfehlungen können Sie die Bearbeitung von Policies vereinfachen:

- + verwenden, um die **Übernehmen**-Markierung für alle Elemente im aktuellen Bereich zu setzen
- Regeln mit dem **Papierkorb**-Symbol löschen

Klicken Sie auf **Intervall ändern**.

Ändern Sie den Wert im Feld **Reguläres Intervall** in den gewünschten Wert für die Intervalldauer (empfohlen: 60 Sekunden) und klicken Sie auf Speichern.

Sobald Sie eine neue Policy für das Agenten-Verbindungsintervall erstellt haben, weisen Sie es zu der statischen Gruppe zu, die Sie in Schritt 1 erstellt haben.

Führen Sie Ihre Tests für die massenhafte Bereitstellung durch und bearbeiten Sie anschließend die Einstellungen der Policy für das Agenten-Verbindungsintervall, das Sie in Schritt 2 erstellt haben.

Klicken Sie auf **Admin** > **Gruppen** und wählen Sie die Registerkarte **Policies** aus. Klicken Sie auf die Policy "Verbindungsintervall für Agent", wählen Sie **Bearbeiten** aus und klicken Sie auf **Einstellungen** > **Verbindung**. Klicken Sie auf **Intervall ändern** und setzen Sie das Verbindungsintervall auf 20 Minuten.

6.1.2.4 Anwenden von Policies auf Clients

Gruppen und Computern können mehrere Policies zugewiesen sein. Ein Computer kann sich außerdem in einer tief verschachtelten Gruppe befinden, deren übergeordnete Gruppen eigene Policies haben.

Die Policies werden gemäß ihrer Reihenfolge angewendet. Die Reihenfolge ergibt sich aus der Reihenfolge der Gruppen und aus der Reihenfolge der einer Gruppe zugewiesenen Policies.

So ermitteln Sie die aktive Policy für einen beliebigen Client:

1. Ermitteln Sie die Reihenfolge der Gruppen, in denen der Client enthalten ist
2. Ersetzen Sie die Gruppen durch die zugewiesenen Policies
3. Führen Sie die Policies zusammen, um die endgültigen Einstellungen zu erhalten

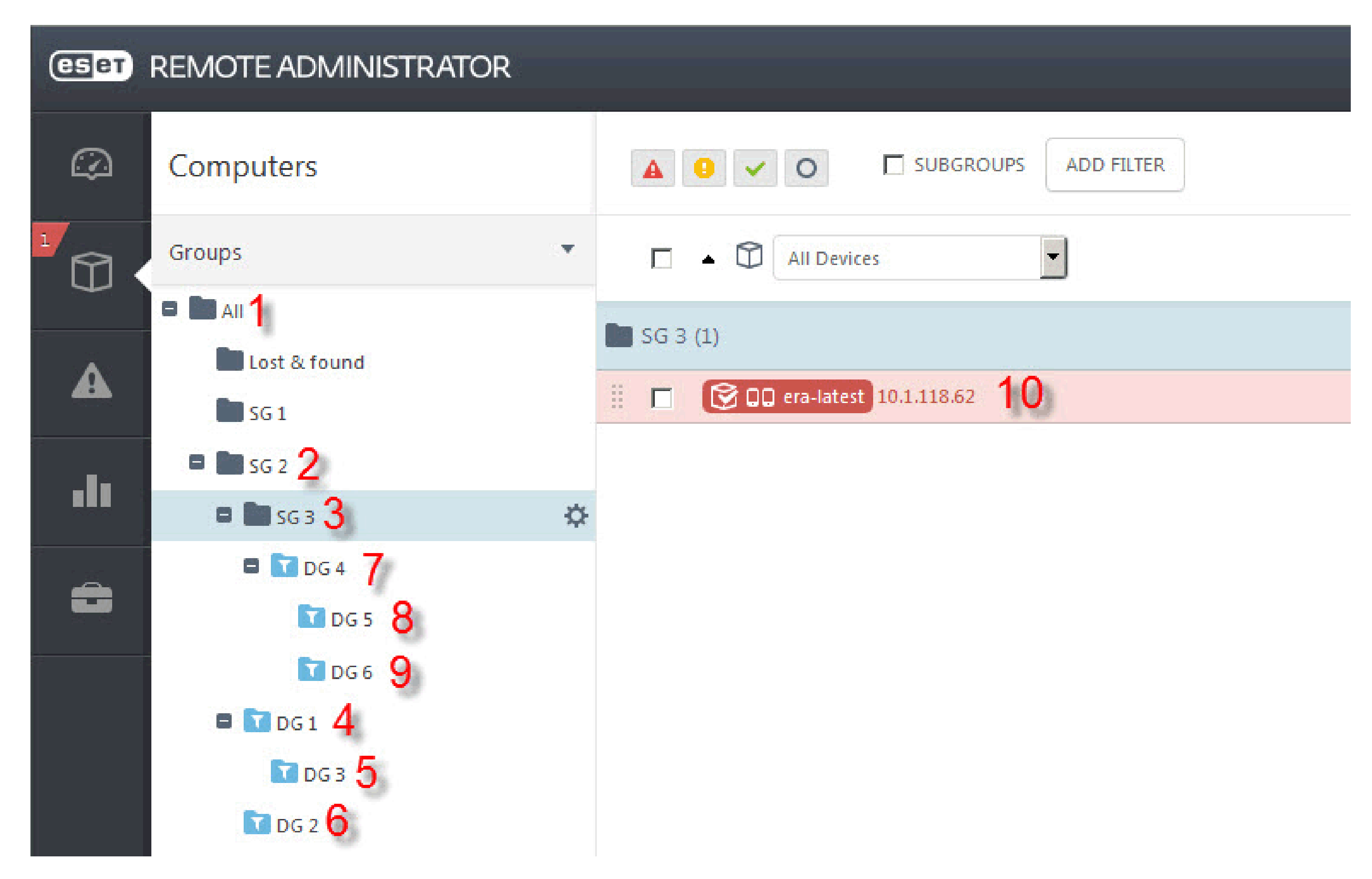
6.1.2.4.1 Ordnen von Gruppen

Policies können **Gruppen** zugewiesen werden und werden in einer bestimmten Reihenfolge angewendet.

Beim Ordnen der Gruppen in der Liste werden mehrere Regeln angewendet:

1. Statische Gruppen werden von der statischen Stammgruppe „Alle“ aus durchlaufen.
2. In jeder Ebene werden die statischen Gruppen der Ebene zuerst in der Reihenfolge durchlaufen, in der sie in der Baumstruktur angezeigt werden (Breitensuche).
3. Nachdem alle statischen Gruppen einer bestimmten Ebene in die Liste aufgenommen wurden, werden die dynamischen Gruppen durchlaufen.
4. In jeder dynamischen Gruppe werden die untergeordneten Gruppen in der Reihenfolge durchlaufen, in der sie in der Liste angezeigt werden.
5. Wenn in einer beliebigen Ebene der dynamischen Gruppen eine untergeordnete Gruppe vorhanden ist, wird sie aufgeführt und nach untergeordneten Elementen durchsucht. Wenn keine weiteren untergeordneten Elemente mehr vorhanden sind, werden die nächsten dynamischen Gruppen der übergeordneten Ebene aufgelistet (Tiefensuche).
6. Das Durchlaufen wird auf Ebene des Computers beendet.

Die folgende Abbildung zeigt diesen Vorgang an einem Beispiel:



Der Stamm (die statische Gruppe „Alle“) wird als **Regel 1** aufgeführt. Da auf der Ebene der Gruppe „Alle“ keine weiteren Gruppen vorhanden sind, werden anschließend die Policies der Gruppen der nächsten Ebene bewertet.

Die Gruppen „Fundbüro“ und die statischen Gruppen SG 1 und SG 2 werden als nächstes bewertet. Der Computer ist nur Mitglied der statischen Gruppen „Alle“/SG 2/SG 3. Die Gruppen „Fundbüro“ und SG 1 müssen daher nicht durchlaufen werden. SG 2 ist die einzige Gruppe auf dieser Ebene, die bewertet wird. Sie wird daher in die Liste aufgenommen. Das Durchlaufen wird eine Ebene tiefer fortgesetzt.

In der dritten Ebene findet der Algorithmus die Gruppen SG 3, DG 1 und DG 2. Gemäß **Regel 2** werden zuerst die statischen Gruppen aufgelistet. Durch das weitere Durchlaufen wird Gruppe SG 3 hinzugefügt. Da dies die letzte statische Gruppe in Ebene 3 ist, wird mit DG 1 fortgefahren. Bevor mit DG 2 in Ebene 3 fortgefahren wird, müssen die untergeordneten Elemente von DG 1 aufgeführt werden.

DG 3 wird hinzugefügt. Diese Gruppe enthält keine untergeordneten Elemente. Daher wird das Durchlaufen auf der nächsthöheren Ebene fortgesetzt.

DG 2 wird aufgeführt. Die Gruppe enthält keine untergeordneten Elemente. In Ebene 3 sind keine weiteren Gruppen vorhanden. Das Durchlaufen wird in Ebene 4 fortgesetzt.

In Ebene 4 befinden sich nur die dynamische Gruppe DG 4 und der Computer selbst. **Regel 6** schreibt vor, dass der Computer als Letztes bearbeitet wird, daher wird DG 4 aufgenommen. DG 4 hat zwei untergeordnete Elemente, die verarbeitet werden müssen, bevor fortgefahren wird.

DG 5 und DG 6 werden zur Liste hinzugefügt. Keine der beiden Gruppen enthält untergeordnete Elemente. Das Durchlaufen ist abgeschlossen. Als Letztes wird der Computer hinzugefügt.

Das Ergebnis ist folgende Liste:

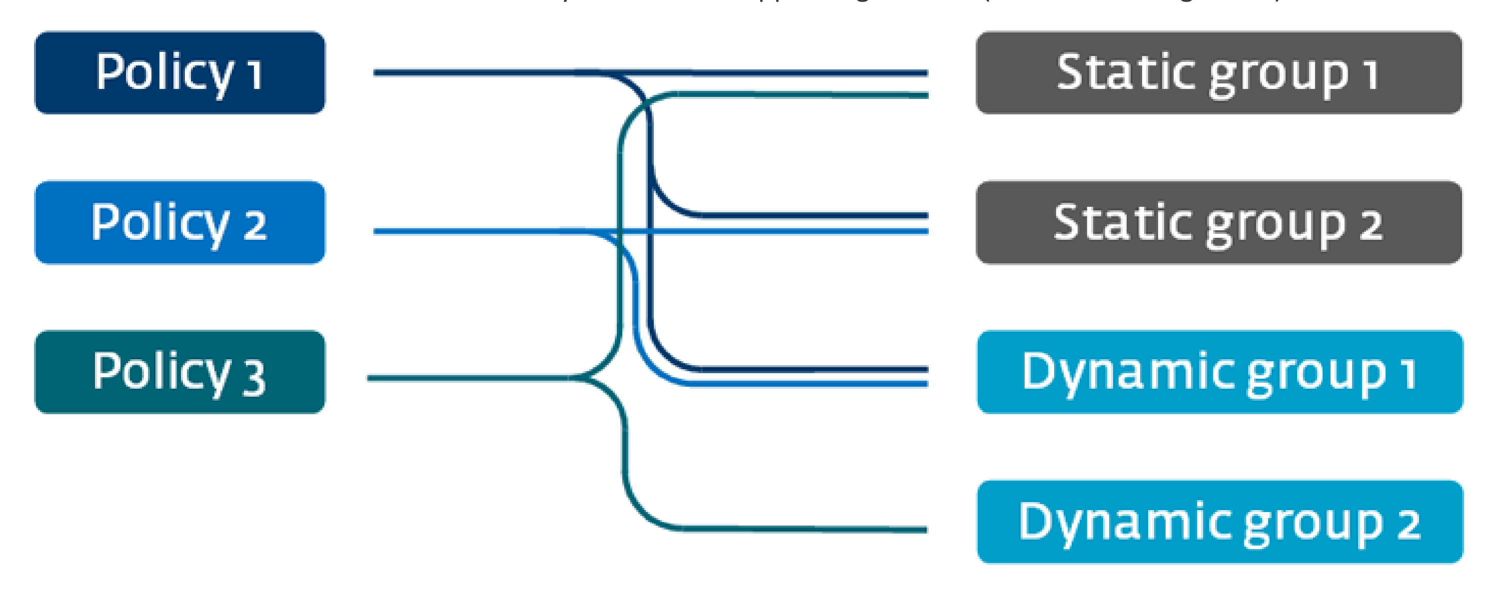
1. Alle
2. SG 2
3. SG 3
4. DG 1
5. DG 3
6. DG 2
7. DG 4
8. DG 5
9. DG 6
10. Computer

Die Policies werden in dieser Reihenfolge angewendet.

6.1.2.4.2 Aufzählen von Policies

Nachdem die Reihenfolge der Gruppen bekannt ist, können Sie die einzelnen Gruppen durch die jeweils zugewiesenen Policies ersetzen. Die Policies werden in der Reihenfolge aufgeführt, in der sie einer Gruppe zugewiesen sind. Gruppen ohne Policy werden aus der Liste entfernt. Für Gruppen mit mehreren zugewiesenen Policies kann die Priorität der Policies bearbeitet werden. Jede Policy konfiguriert nur ein Produkt (ERA-Agent, ERA-Proxy, EES, usw.)

3 Policies sind sowohl statischen als auch dynamischen Gruppen zugewiesen (siehe Abbildung unten):



Unsere Liste aus Schritt 1 würde folgendermaßen verändert:

1. Alle (entfernt, keine Policy)
2. SG 2 -> Policy 1, Policy 2
3. SG 3 (entfernt, da keine Policy)
4. DG 1 -> Policy 1, Policy 2
5. DG 3 (entfernt, keine Policy)
6. DG 2 -> Policy 3
7. DG 4 (entfernt, keine Policy)
8. DG 5 (entfernt, keine Policy)
9. DG 6 (entfernt, keine Policy)
10. Computer (entfernt, keine Policy)

Die endgültige Liste der Policies ist:

1. Policy 1
2. Policy 2
3. Policy 1
4. Policy 2
5. Policy 3

6.1.2.4.3 Zusammenführen von Policies

Policies werden einzeln zusammengeführt. Beim Zusammenführen von Policies gilt die allgemeine Regel, dass die letzte Policy jeweils die Einstellungen der vorigen Policy ersetzt.
Um dieses Verhalten zu ändern, können Sie Policy-Markierungen verwenden (für jede Einstellung verfügbar). Die Einstellungen werden einzeln zusammengeführt.

Beachten Sie, dass die Struktur der Gruppen (ihre Hierarchie) und die Reihenfolge der Policies festlegen, wie die Policies zusammengeführt werden. Das Zusammenführen von zwei Policies kann je nach Reihenfolge der Policies zu einem unterschiedlichen Ergebnis führen. Die Gruppen wurden sortiert und die Policies aufgezählt.

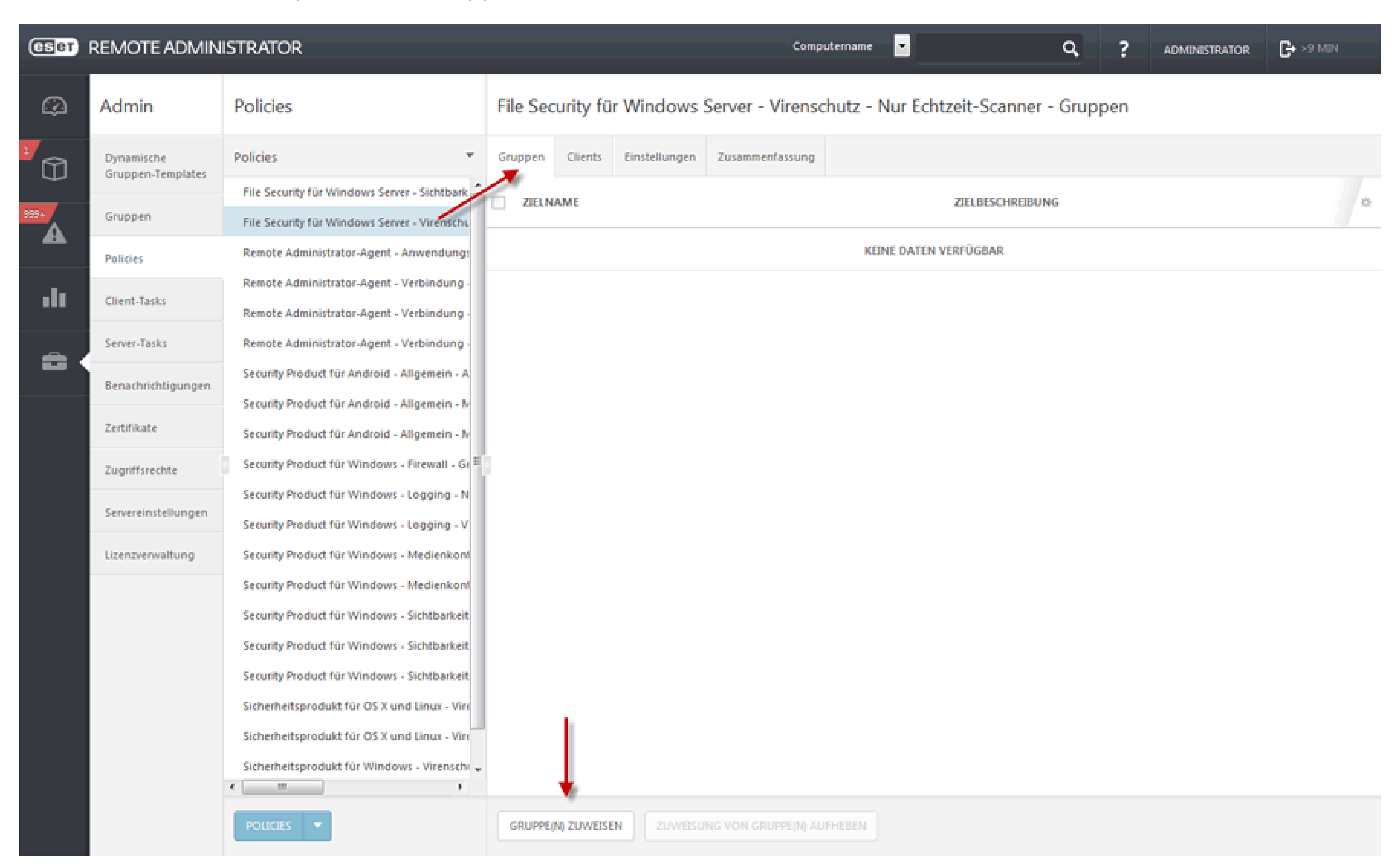
6.1.2.5 Konfiguration eines Produkts über ERA

Mit Policies können Sie Ihr ESET-Produkt auf die gleiche Weise konfigurieren, wie über das Fenster für die erweiterten Einstellungen in der Benutzeroberfläche des Produkts. Anders als Policies in Active Directory können ERA-Policies keine Skripte oder Befehlsfolgen enthalten.

6.1.2.6 Zuweisen einer Policy zu einer Gruppe

Nachdem Sie eine Policy erstellt haben, können Sie sie einer **statischen** oder **dynamischen Gruppe** zuweisen. Es gibt zwei Möglichkeiten zum Zuweisen einer Policy:

1. Klicken Sie auf **Admin** > **Policies**, wählen Sie eine Policy aus und klicken Sie auf **Gruppe(n) zuweisen**. Wählen Sie eine statische oder dynamische Gruppe aus und klicken Sie auf **OK**.



Wählen Sie **Gruppe** in der Liste aus.

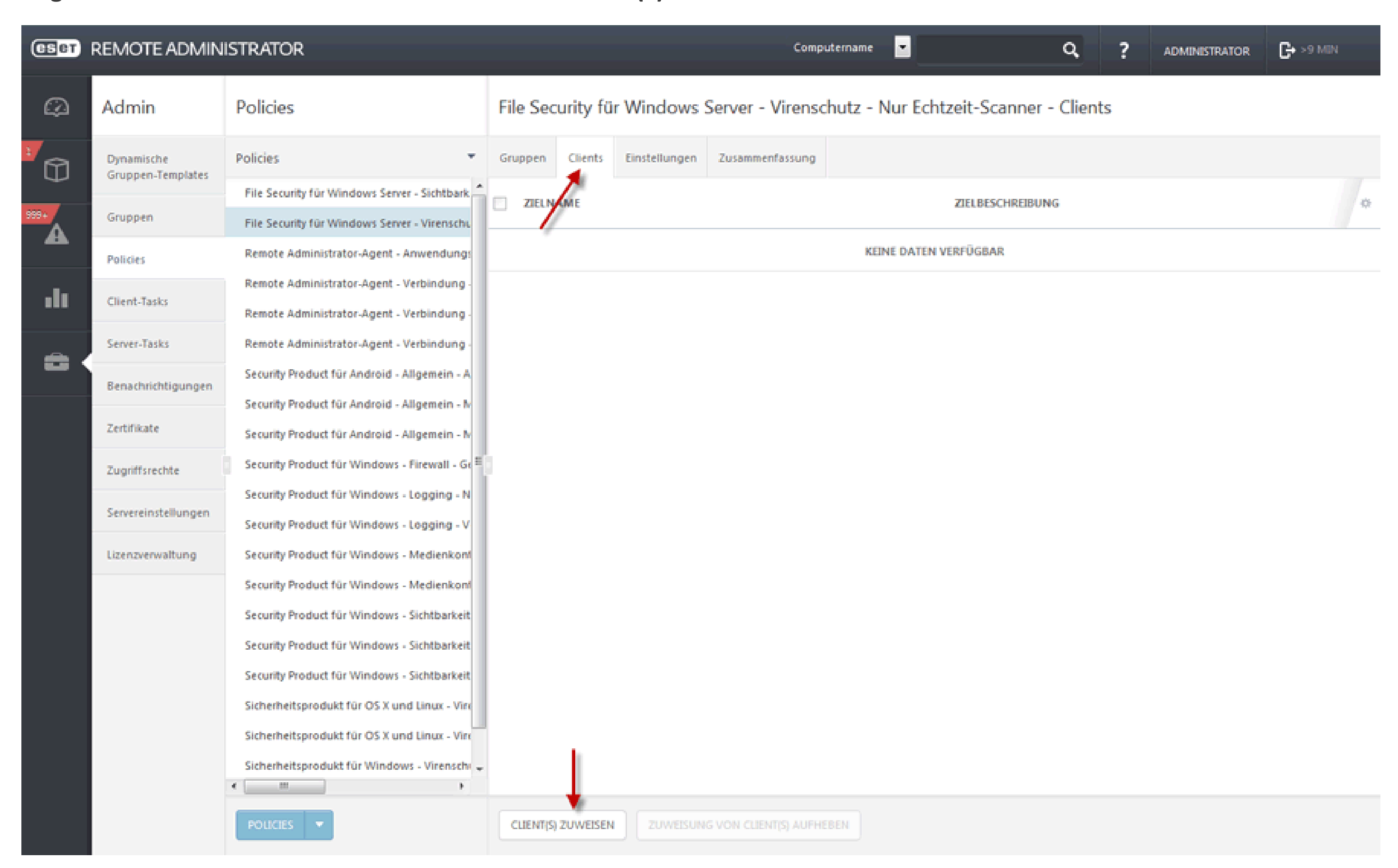
2. Klicken Sie auf **Admin** > **Gruppen** > **Gruppe** oder neben dem Gruppennamen auf das Zahnradsymbol ⚙. Wählen Sie **Policies** verwalten aus.

Klicken Sie im Fenster **Anwendungsreihenfolge für Policies** auf **Policy hinzufügen**. Aktivieren Sie das Kontrollkästchen neben der Policy, die Sie der Gruppe zuweisen möchten, und klicken Sie auf **OK**.
Klicken Sie auf **Speichern**. Um anzuzeigen, welche Policies einer bestimmten Gruppe zugewiesen sind, wählen Sie die gewünschte Gruppe aus und klicken Sie auf die Registerkarte **Policies**. Eine Liste der Policies, die dieser Gruppe zugewiesen sind, wird angezeigt.

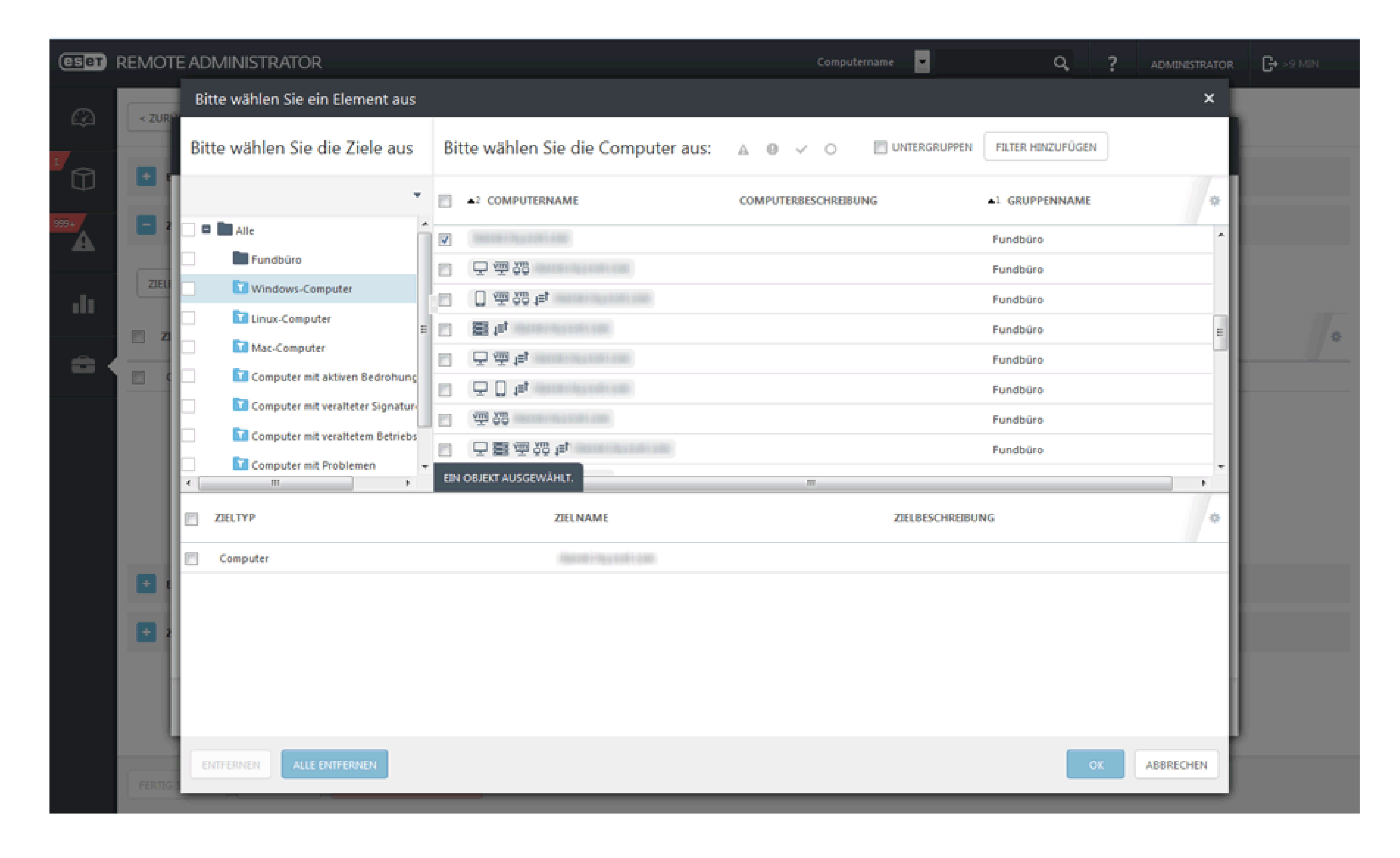
HINWEIS: Weitere Informationen zu Policies finden Sie im Kapitel Policies.

6.1.2.7 Zuweisen einer Policy zu einem Client

Um eine Policy zu einer Clientarbeitsstation zuzuweisen, klicken Sie auf **Admin** > **Policies** und wählen Sie die Registerkarte **Clients** aus. Klicken Sie dann auf **Client(s) zuweisen**.



Wählen Sie den oder die Zielclientcomputer aus und klicken Sie auf **OK**. Die Policy wird allen ausgewählten Computern zugewiesen.



6.1.3 Client-Tasks

Mit einem **Clienttask** können Sie eine Aktion von einem Clientcomputer anfordern. Client-Tasks können Gruppen oder einzelnen Computern zugewiesen werden. Nachdem ein Task erstellt wurde, wird er gemä´des Zeitplans ausgeführt. Da die Clients nicht ständig mit dem ERA-Server verbunden sind, kann es eine Weile dauern, bis Tasks an alle Clients verteilt sind. Aus dem gleichen Grund kann es auch eine gewisse Zeit dauern, bis die Ergebnisse der Taskausführung auf dem ERA-Server empfangen werden. Folgende vordefinierte Tasks stehen Ihnen zur einfacheren Verwendung zur Verfügung:

Jede **Taskkategorie** enthält **Tasktypen:**

Alle Tasks

⊟ **ESET-Sicherheitsprodukt**

Konfiguration verwalteter Produkte exportieren

On-Demand-Prüfung

Produktaktivierung

Quarantäneverwaltung

SysInspector-Skript ausführen

SysInspector-Loganfrage

Quarantänedatei hochladen

Update der Signaturdatenbank

Rollback eines Updates der Signaturdatenbank

⊟ **ESET Remote Administrator**

Upgrade von Remote Administrator-Komponenten

Geklonten Agenten zurücksetzen

Rogue Detection Sensor-Datenbank zurücksetzen

Verwaltung beenden (ERA-Agent deinstallieren)

Betriebssystem

Meldung anzeigen

Betriebssystem-Update

Befehl ausführen

Software-Installation

Software-Deinstallation

Verwaltung beenden (ERA-Agent deinstallieren)

Mobilgerät

Anti-Theft-Aktion

Geräteregistrierung

Meldung anzeigen

Konfiguration verwalteter Produkte exportieren

On-Demand-Scan

Produktaktivierung

Software-Installation

Update der Signaturdatenbank

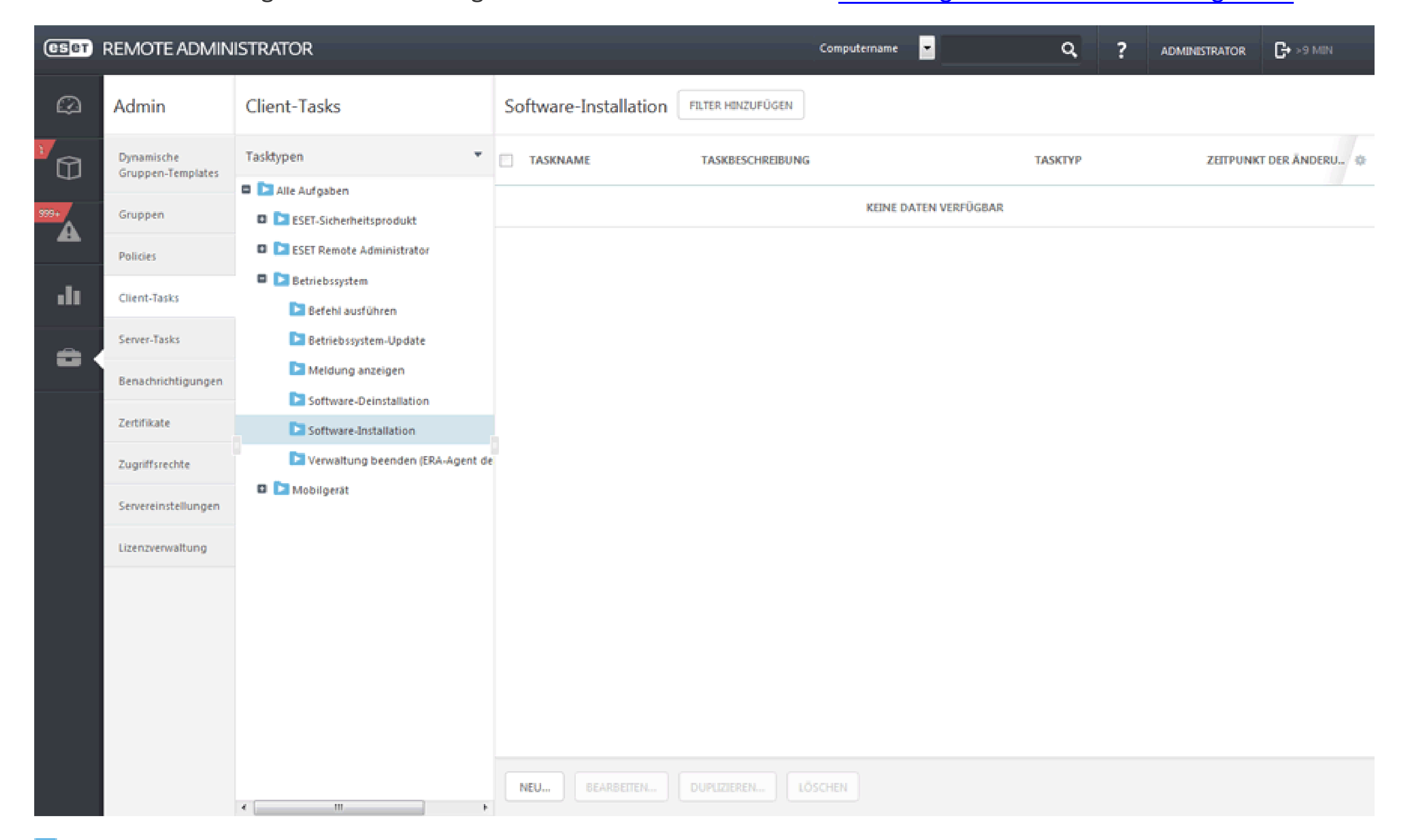
Verwaltung beenden (ERA-Agent deinstallieren)

6.1.3.1 Assistent für Client-Tasks

Client-Tasks werden über die Registerkarte **Admin** erstellt und verwaltet. Klicken Sie auf **Client-Tasks**, wählen Sie in der Liste **Tasktypen** einen Task aus und klicken Sie dann auf **Neu**.

ESET-Sicherheitsprodukte können remote installiert werden. Klicken Sie hierzu auf den gewünschten Computer und wählen Sie **Neu** aus oder erstellen Sie einen neuen Task **Software-Installation** im Menü **Admin** > **Client-Tasks**. Klicken Sie auf **Neu...**, um mit der Einrichtung des neuen Tasks zu beginnen.

- Führen Sie die folgenden Anweisungen aus oder sehen Sie sich das Anleitungsvideo in der Knowledgebase an.



Basis

Geben Sie grundlegende Informationen zum Task ein, wie **Name** und fakultativ eine **Beschreibung** und den **Tasktyp**. Der **Tasktyp** (siehe Liste oben) legt die Einstellungen und das Verhalten des Tasks fest. Wählen Sie den Task **Software-Installation** aus und klicken Sie dann auf **Ziel**.

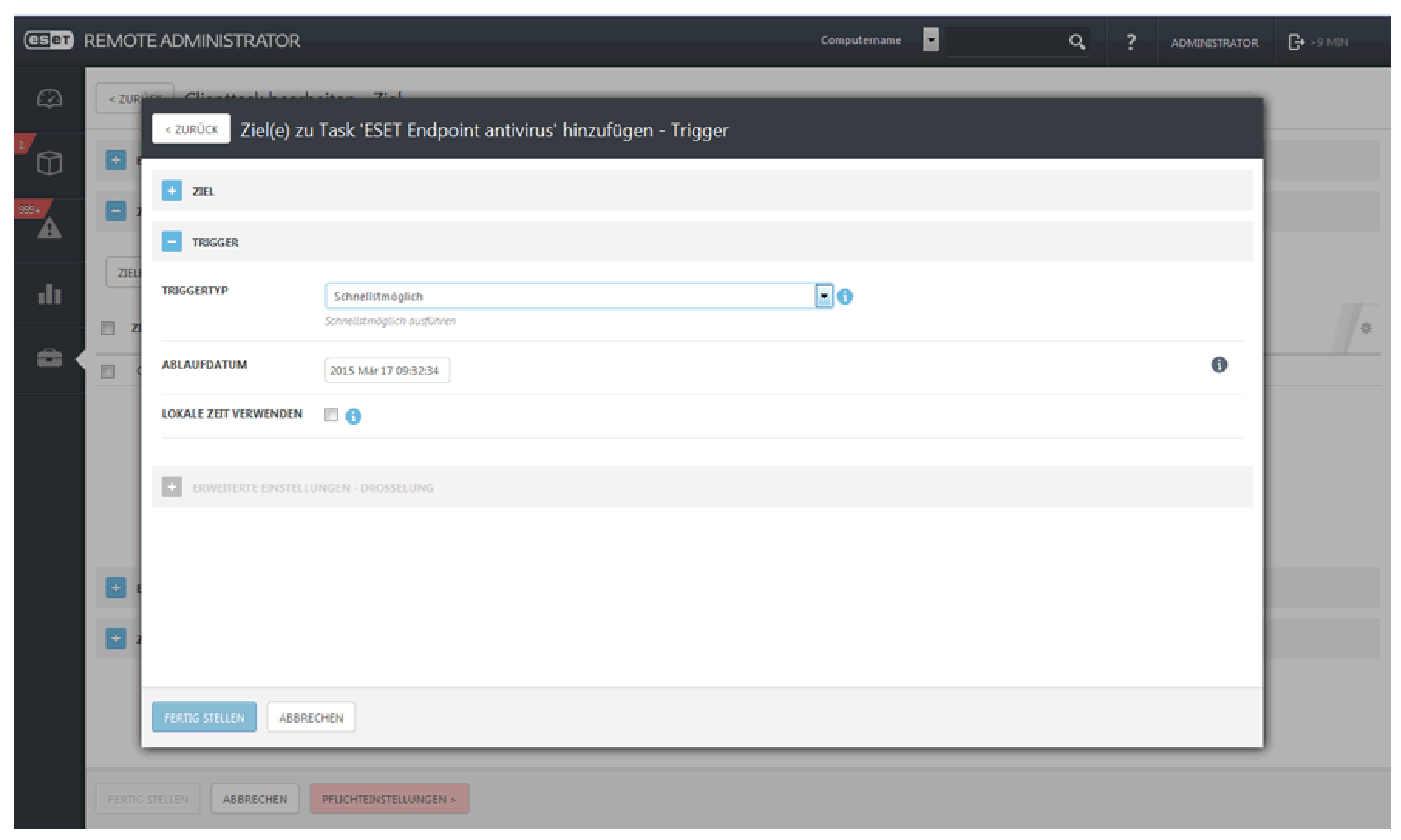
Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die den Task empfangen sollen.

Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.

Trigger

Als **Trigger** wählen Sie „Schnellstmöglich ausführen“ aus. Damit wird der Tasks sofort zu den Clients gesendet. Die Option **Lokale Zeit verwenden** bezieht sich auf die lokale Zeit auf dem Clientsystem, nicht auf dem Server.



Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Trigger bei Aufnahme in dynamische Gruppe** (siehe oben). Lassen Sie die Option Drosselung zunächst unverändert. Klicken Sie auf „Fertig stellen“, um den neuen Task zu erstellen.

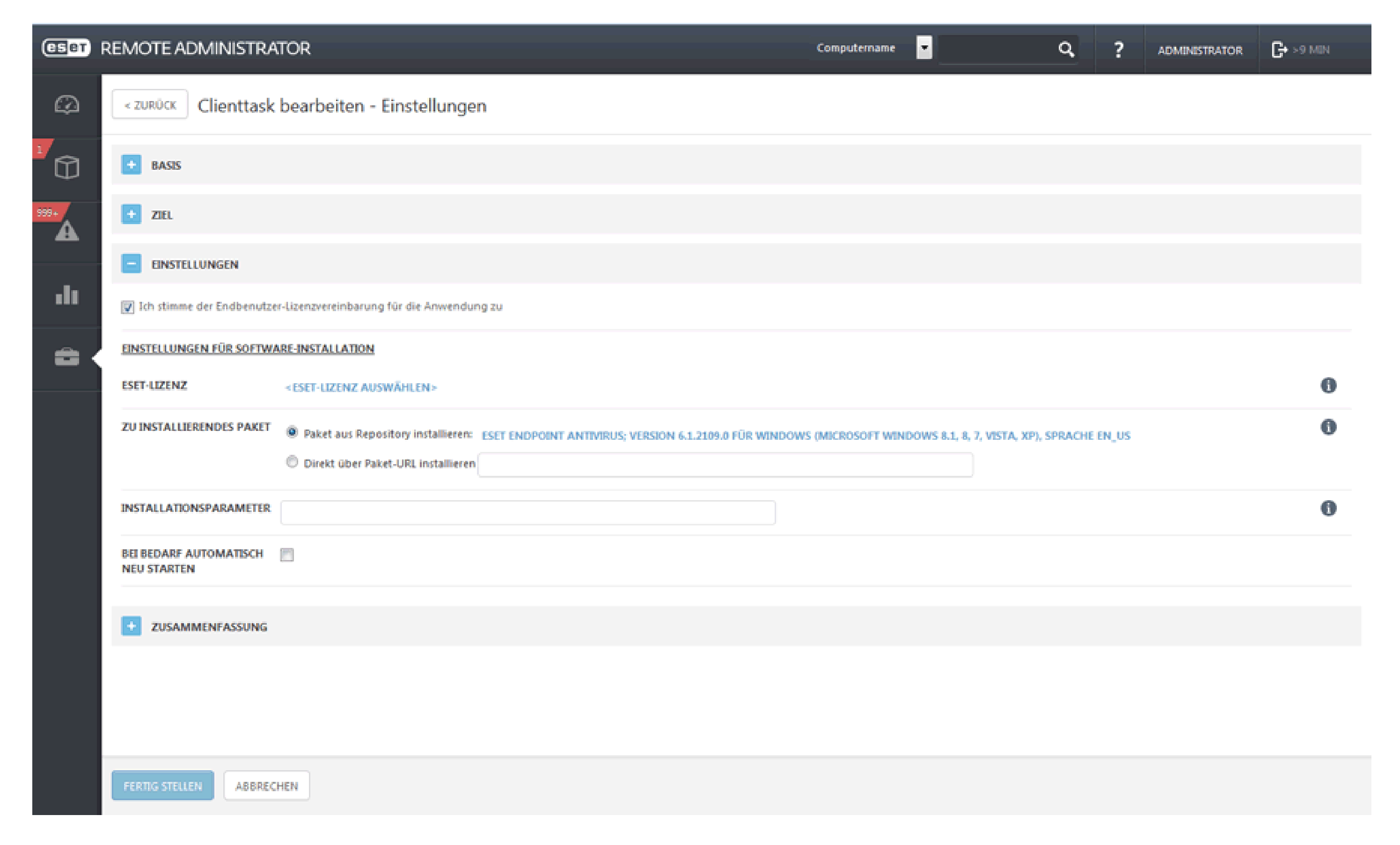
Einstellungen

Klicken Sie auf **<ESET-Lizenz auswählen>** und wählen Sie aus der Liste der verfügbaren Lizenzen die geeignete Lizenz für das installierte Produkt aus. Aktivieren Sie das Kontrollkästchen neben **Ich stimme der Endbenutzer-Lizenzvereinbarung für die Anwendung zu**, sofern Sie zustimmen. Weitere Informationen hierzu finden Sie unter Lizenzverwaltung oder EULA.

Klicken Sie auf **<Paket auswählen>**, um ein Installationspaket aus dem Repository auszuwählen, oder geben Sie eine Paket-URL ein. Eine Liste verfügbarer Pakete wird angezeigt, in der Sie das zu installierende ESET-Produkt (zum Beispiel ESET Endpoint Security) auswählen können. Wählen Sie das gewünschte Installationspaket aus und klicken Sie auf **OK**. Wenn Sie eine URL für das Installationspaket angeben möchten, geben Sie die URL durch Eintippen oder Kopieren und Einfügen in das Textfeld ein (verwenden Sie keine URLs, die Authentifizierung erfordern).

HINWEIS: Beachten Sie, dass Server und Agent mit dem Internet verbunden sein müssen, um auf das Repository zugreifen und die Installation durchführen zu können. Falls Sie keinen Internetzugriff haben, können Sie die Clientsoftware lokal installieren.

Bei Bedarf können Sie Installationsparameter angeben. Andernfalls lassen Sie dieses Feld leer. Aktivieren Sie das Kontrollkästchen neben Bei Bedarf automatisch neu starten, um einen automatischen Neustart des Computers nach der Installation zu erzwingen. Sie können diese Option auch deaktiviert lassen. Die Entscheidung über den Neustart wird dann vom Benutzer des Clientcomputers getroffen.



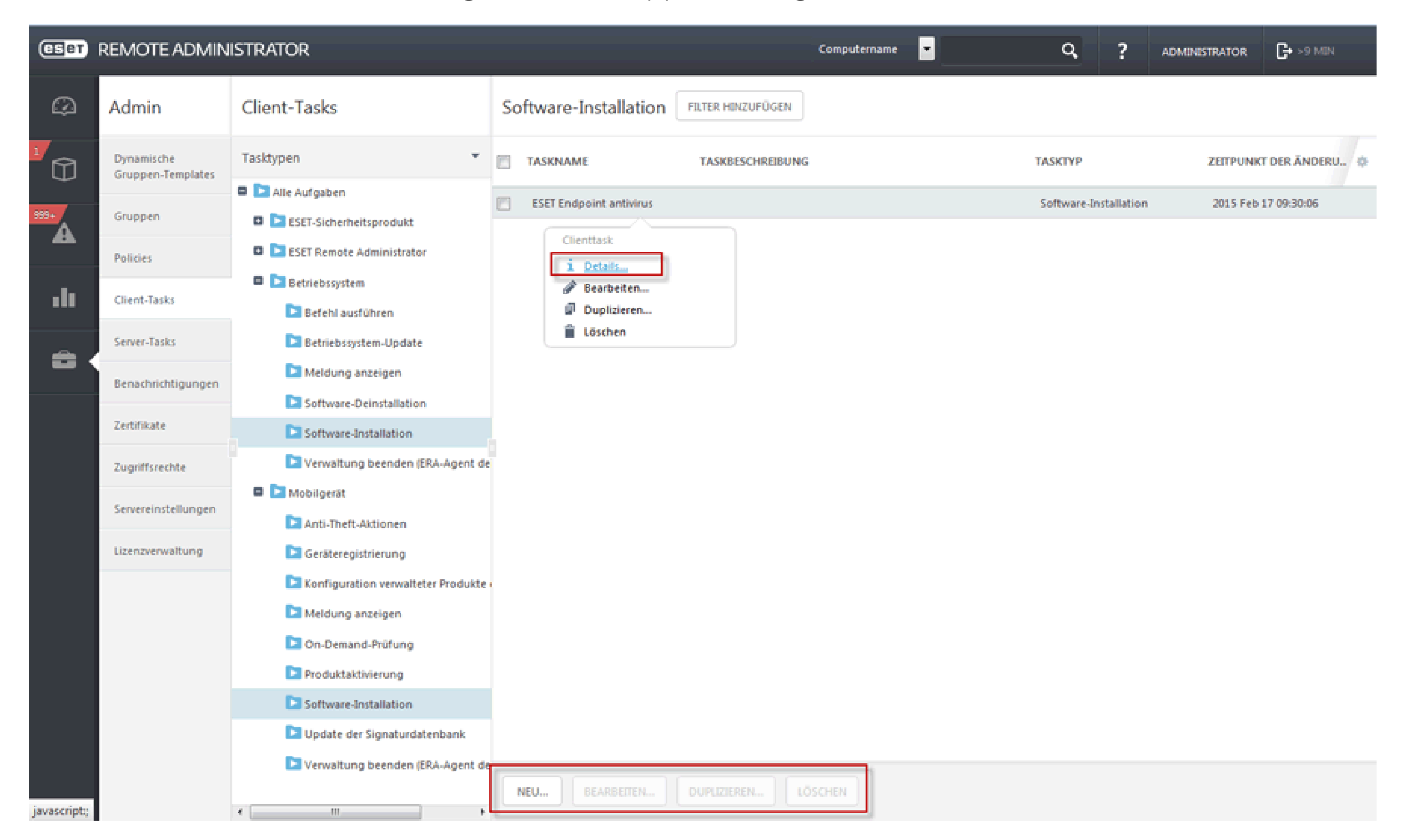
Zusammenfassung

Überprüfen Sie die Zusammenfassung der konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**. Der Task ist jetzt erstellt und wird an den/die Client(s) gesendet.

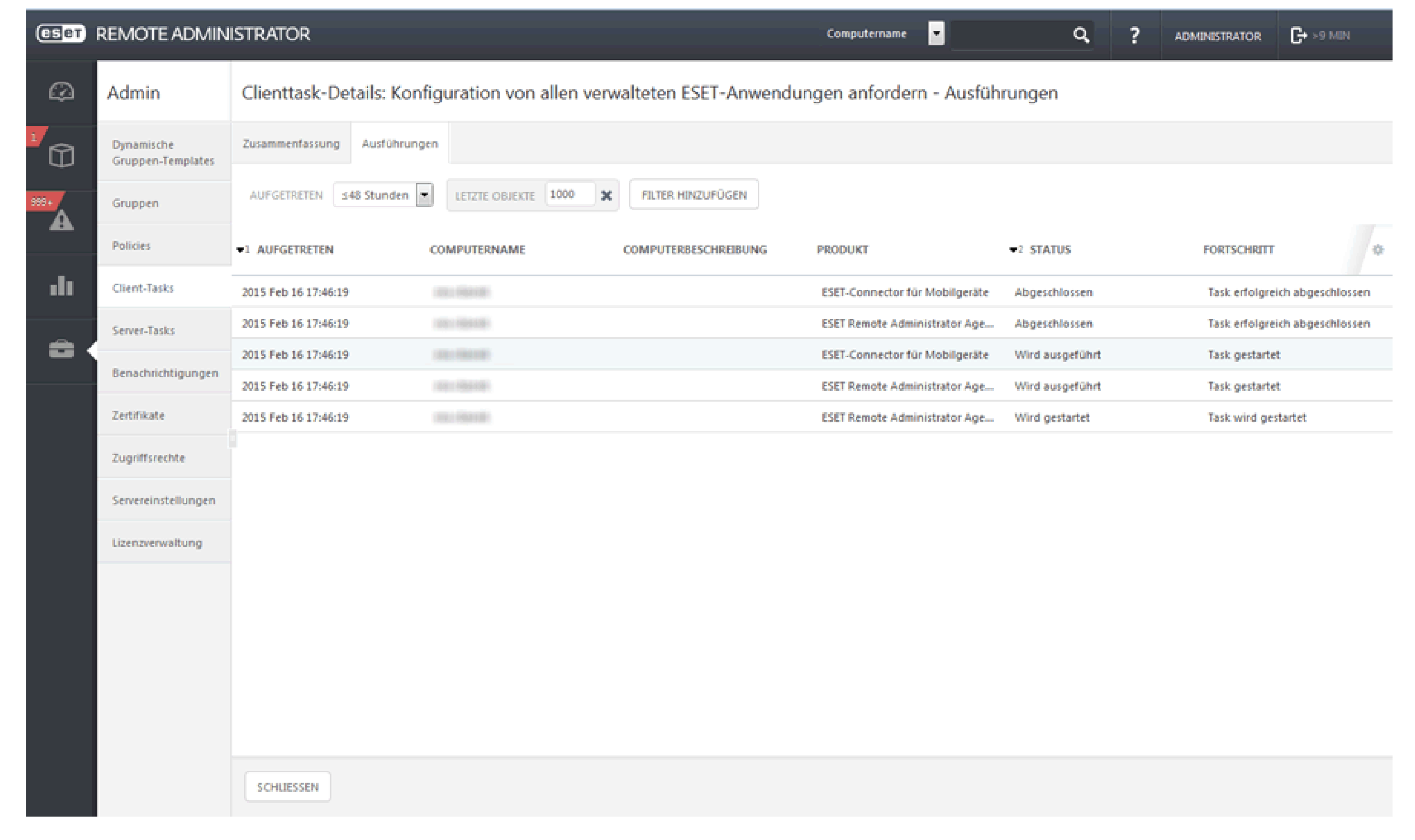
6.1.3.2 Verwalten von Client-Tasks

Mit Client-Tasks können Sie Clients und deren Sicherheitsprodukte verwalten. Ein Satz vordefinierter Tasks deckt die häufigsten Verwendungszwecke ab. Alternativ können Sie benutzerdefinierte Tasks mit besonderen Einstellungen erstellen.

- Sie können vorhandene Tasks mit der Funktion **Bearbeiten** ändern, um neue Tasks zu erstellen. Das Bearbeiten eines vorhandenen Tasks ist sinnvoll, wenn Sie nur geringfügige Änderungen vornehmen möchten. Wenn Sie Tasks mit völlig anderen Einstellungen verwenden möchten, empfiehlt es sich, stattdessen von Grund auf einen neuen Task zu erstellen.
- **Duplizieren -** Ein neuer Clienttask wird auf Grundlage des ausgewählten Tasks hinzugefügt. Für den neuen Task muss ein Name angegeben werden.
- **Löschen -** Entfernt den oder die ausgewählten Task(s) vollständig.



- **Details ...** - enthält die Taskkonfiguration, eine **Zusammenfassung** und die **Ausführungen des Tasks.** (Aufgetreten, Computername, Produkt, Status und Fortschritt).



HINWEIS: Wenn ein älteres Produkt installiert wird, zeigt der Clienttaskbericht die Information „Task wurde an verwaltetes Produkt übergeben“ an.

6.1.3.2.1 On-Demand-Scan

Mit dem Task **On-Demand-Scan** können Sie manuell einen Scan des Clientcomputers starten (unabhängig von den regulär geplanten Scans).

Nach Scan herunterfahren - Wenn Sie diese Option aktivieren, wird der Computer nach dem Fertigstellen des Scans automatisch heruntergefahren.

Prüfprofil - Wählen Sie aus dem Dropdownmenü das gewünschte Profil aus:

- **Tiefen-Scan** – Dies ist ein auf dem Client vordefiniertes Profil zum Ausführen eines besonders gründlichen Scans. Das gesamte System wird gescannt, der Scan nimmt jedoch auch am meisten Zeit und Ressourcen in Anspruch.
- **Smart-Prüfung -** Mit dem Smart-Scan können Sie schnell den Computer scannen und infizierte Dateien entfernen, ohne eingreifen zu müssen. Ihr Vorteil ist die einfache Bedienung, bei der Sie keine detaillierten Prüfeinstellungen festlegen müssen. Bei der Smart-Prüfung werden alle Dateien auf allen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt.
- **Scan aus Kontextmenü** - Führt auf dem Client ein Scan mit einem vordefinierten Scanprofil aus. Sie können die zu scannenden Objekte benutzerdefiniert anpassen.
- **Benutzerdefiniertes Profil** – Beim Prüfen mit speziellen Einstellungen können Sie verschiedene Prüfparameter festlegen, z. B. die zu prüfenden Objekte und die Prüfmethoden. Der Vorteil eines benutzerdefinierten Scans ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden. Das ist hilfreich, um Prüfungen wiederholt mit denselben Parametern auszuführen. Bevor der Task mit der Option „benutzerdefiniertes Profil“ ausgeführt werden kann, muss ein Profil erstellt werden. Nachdem Sie im Dropdownmenü ein benutzerdefiniertes Profil ausgewählt haben, geben Sie im Feld **Benutzerdefiniertes Profil** den genauen Profilnamen ein.

Säubern

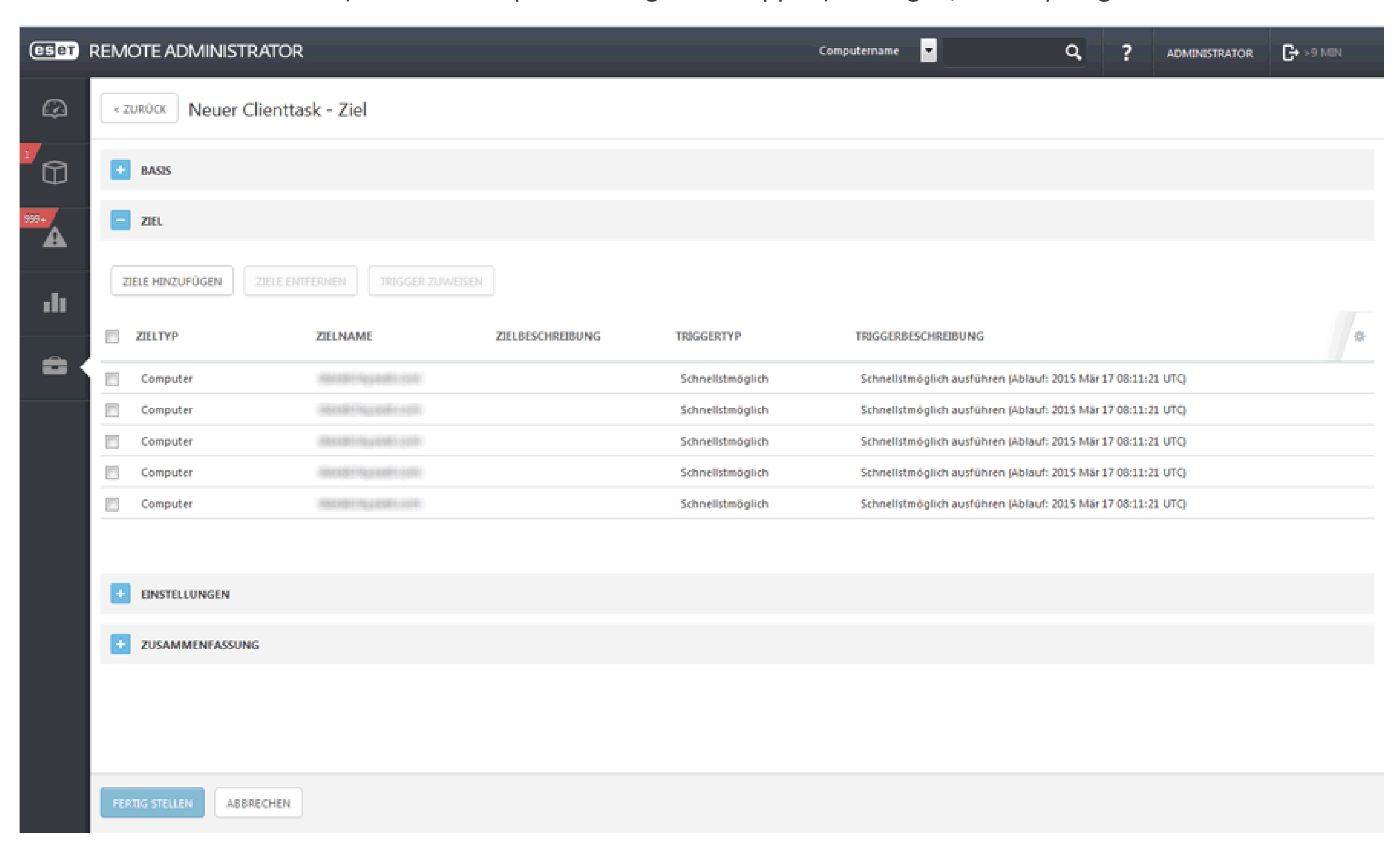
Standardmäßig ist **Prüfen und Aktion** ausgewählt. Hierbei werden gefundene infizierte Objekte automatisch gesäubert. Wenn dies nicht möglich ist, werden sie in die Quarantäne verschoben.

Prüfungsziele

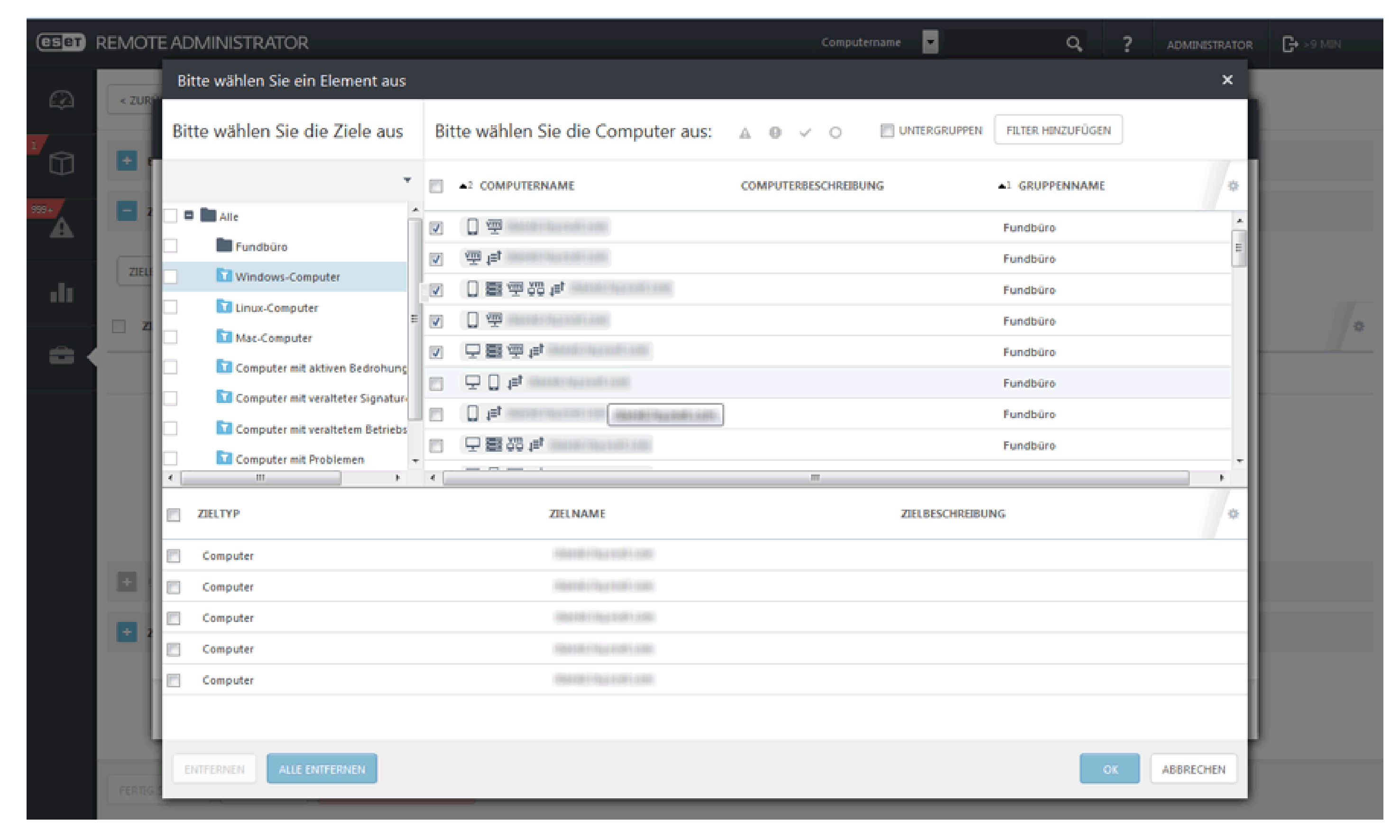
Diese Option ist ebenfalls standardmäßig aktiviert. Mit dieser Einstellung werden alle im Prüfprofil festgelegten Ziele geprüft. Wenn Sie die Option deaktivieren, müssen Sie im Feld **Ziel hinzufügen** manuell die zu scannenden Objekte angeben. Geben Sie das zu scannende Objekt ein und klicken Sie auf **Hinzufügen**. Das Ziel wird im Feld der Prüfziele angezeigt.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Zusammenfassung

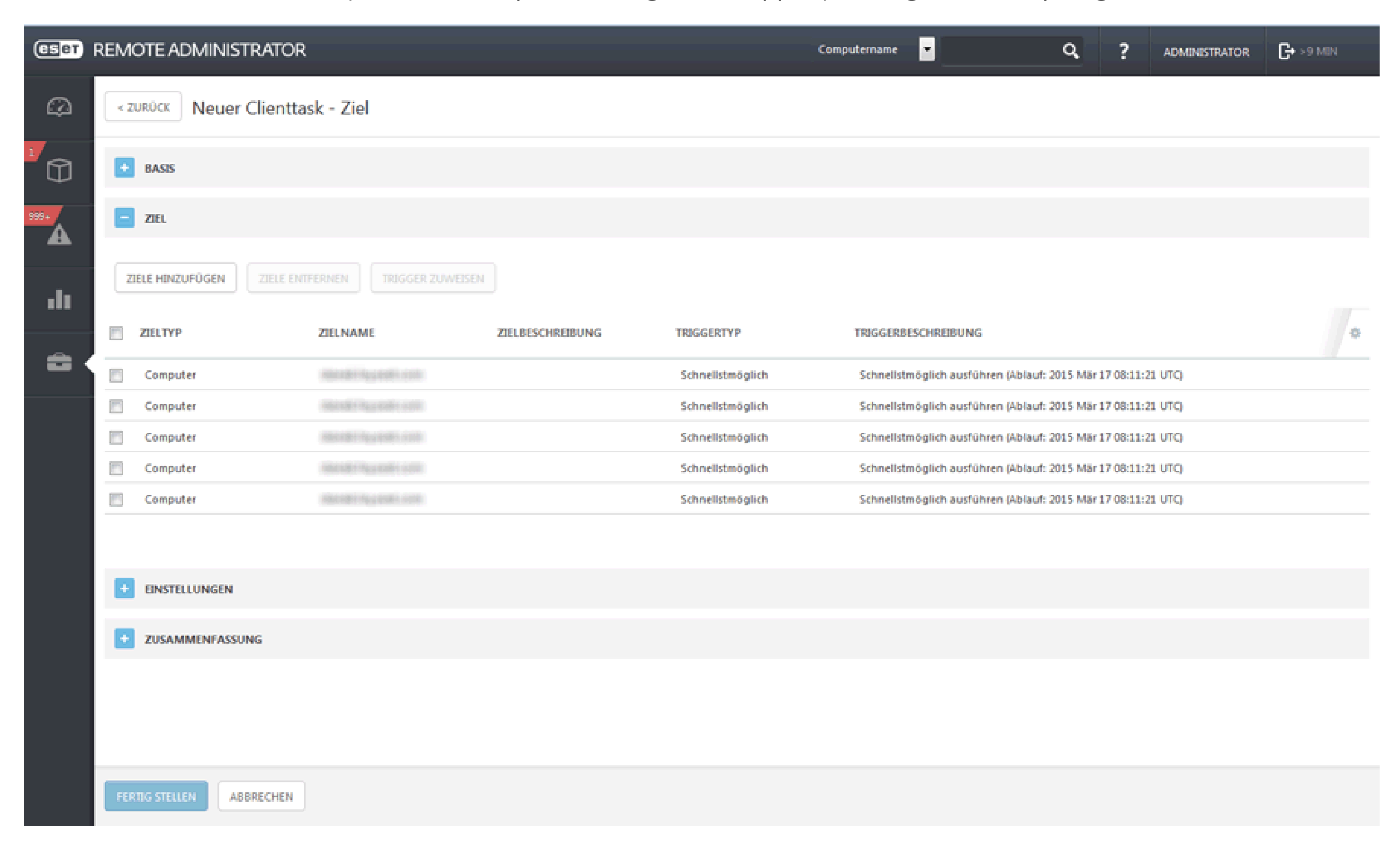
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.2 Betriebssystem-Update

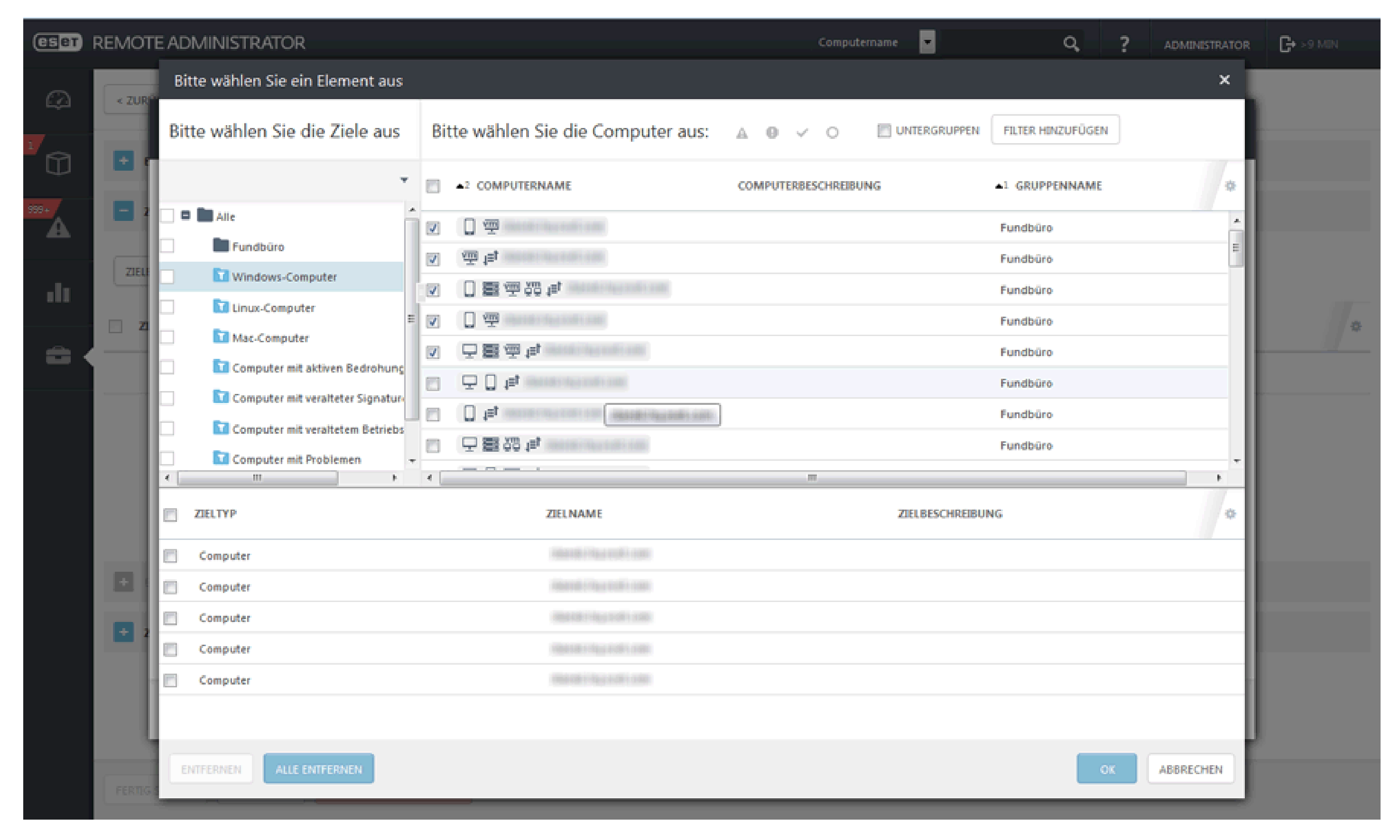
Der Task **System-Update** dient dem Aktualisieren des Betriebssystems auf dem Clientcomputer. Der Task kann Updates für Windows-, Mac- oder Linux-Betriebssysteme auslösen.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Neustart zulassen** – Diese Option gilt nur für Windows-Betriebssysteme und lässt zu, dass der Clientcomputer nach der Installation eines Updates neu gestartet wird.

Zusammenfassung

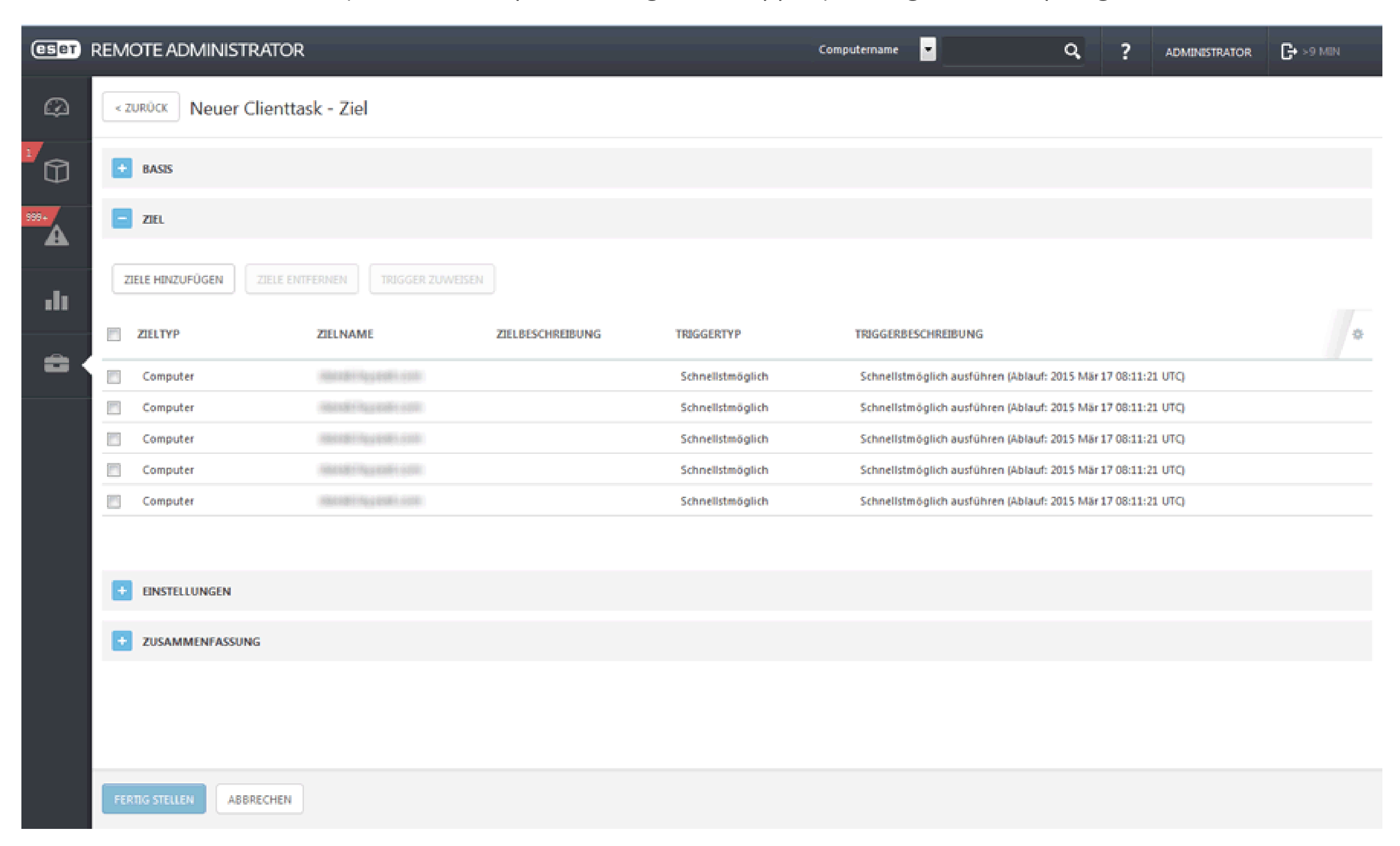
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.3 Quarantäneverwaltung

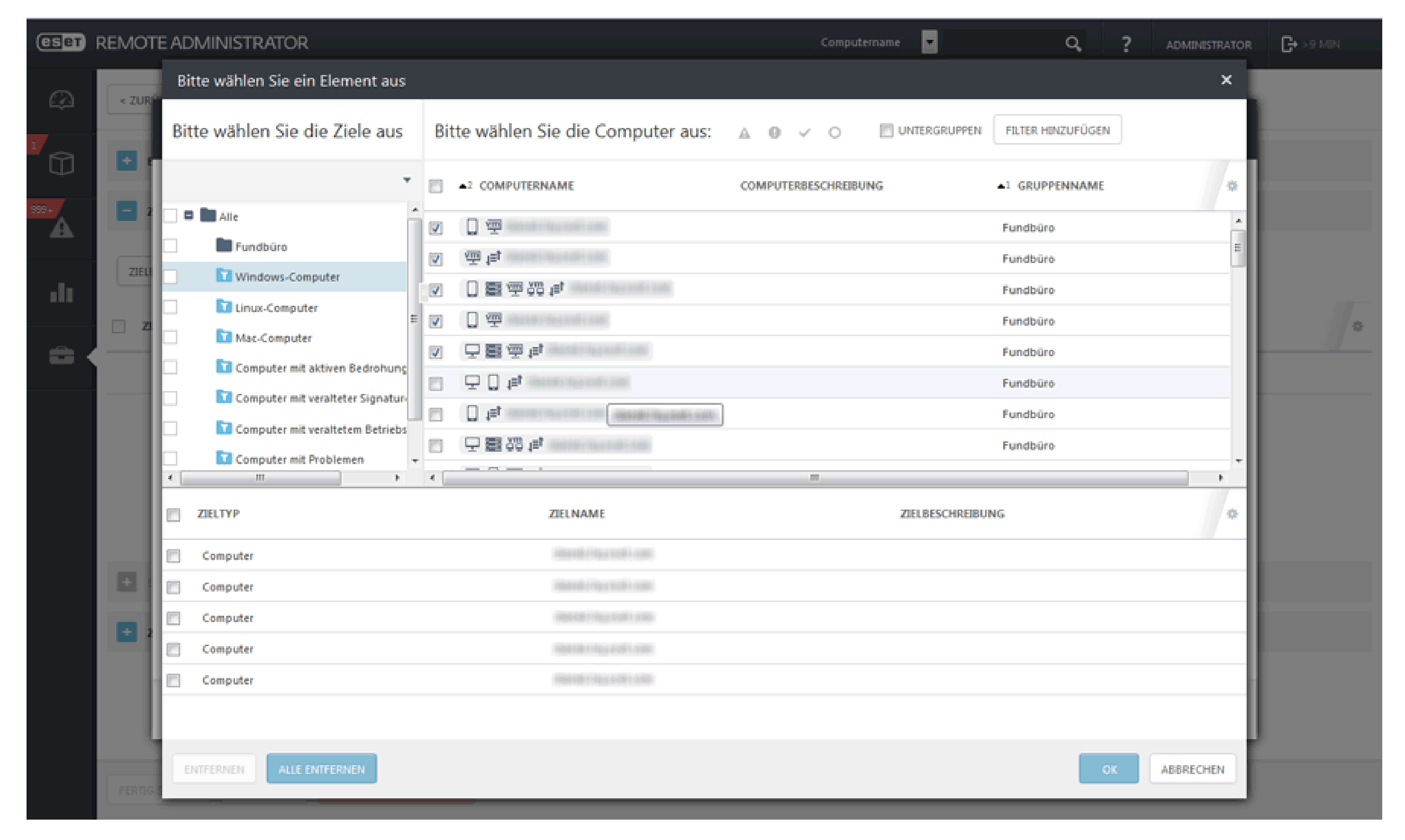
Mit dem Task **Quarantäneverwaltung** werden die Objekte in der Quarantäne des ERA-Servers verwaltet. Hierbei handelt es sich um infizierte oder verdächtige Objekte, die während einer Prüfung erkannt wurden.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Quarantäneverwaltungseinstellungen

- **Aktion** – Wählen Sie die Aktion aus, die auf das Objekt in der Quarantäne angewendet werden soll.

Objekt wiederherstellen (stellt das Objekt am ursprünglichen Speicherort wieder her; das Objekt wird jedoch gescannt und bei Fortbestehen des Quarantänegrunds erneut in die Quarantäne verschoben)
Objekt wiederherstellen und in Zukunft ausschließen (stellt das Objekt am ursprünglichen Speicherort wieder her und verschiebt es nicht mehr in die Quarantäne)
Objekt löschen (löscht das Objekt).

- **Filtertyp** – Sie können die Objekte in der Quarantäne mit den unten angegebenen Kriterien filtern. Der Filter kann entweder auf der Hash-Zeichenkette des Objekts oder auf Bedingungen basieren.

Einstellungen für Hashfilter

Fügen Sie in das Feld Hash-Elemente ein. Es können nur bekannte Objekte eingegeben werden, beispielsweise ein Objekt, das bereits in die Quarantäne verschoben wurde.

Bedingte Filtereinstellungen

- **Aufgetreten von/bis** – Legen Sie hier den Zeitraum fest, in dem das Objekt in die Quarantäne verschoben wurde.
- **Mindestgröße/Maximalgröße (Byte)** – Legen Sie hier den Größenbereich für das in die Quarantäne verschoben Objekt (in Byte) fest.
- **Bedrohungsname** – Wählen Sie aus der Liste der Objekte in der Quarantäne eine Bedrohung aus.
- **Objektname** – Wählen Sie aus der Liste der Objekte in der Quarantäne ein Objekt aus.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen", wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

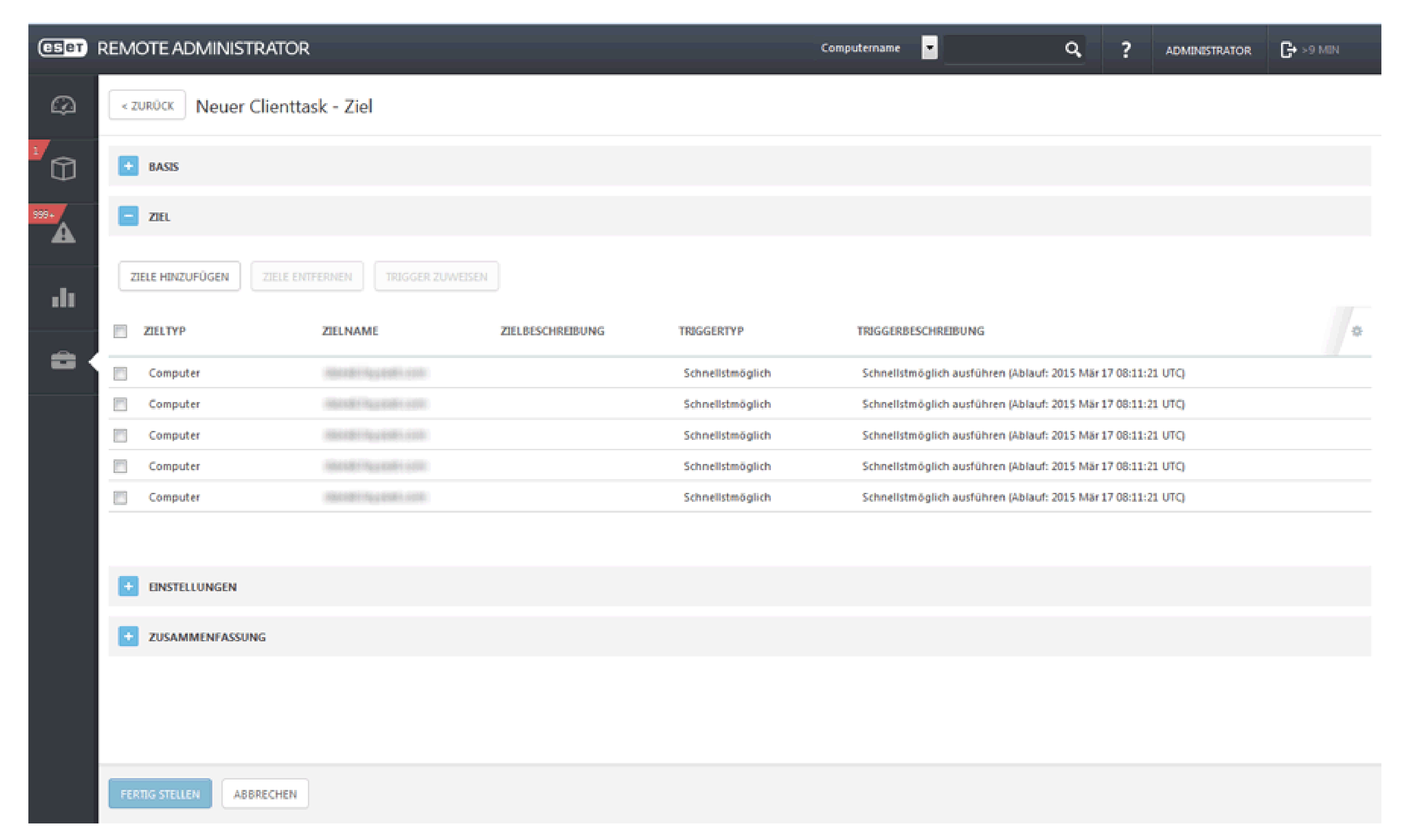
6.1.3.2.4 Rogue Detection Sensor-Datenbank zurücksetzen

Der Task **Rogue Detection Sensor-Datenbank zurücksetzen** setzt den Cache der RD Sensor-Suchen zurück. Der Task löscht den Cache und die Suchergebnisse werden erneut gespeichert. Der Task entfernt keine erkannten Computer. Dieser Task ist hilfreich, wenn erkannte Computer noch im Cache vorhanden sind und nicht dem Server gemeldet werden.

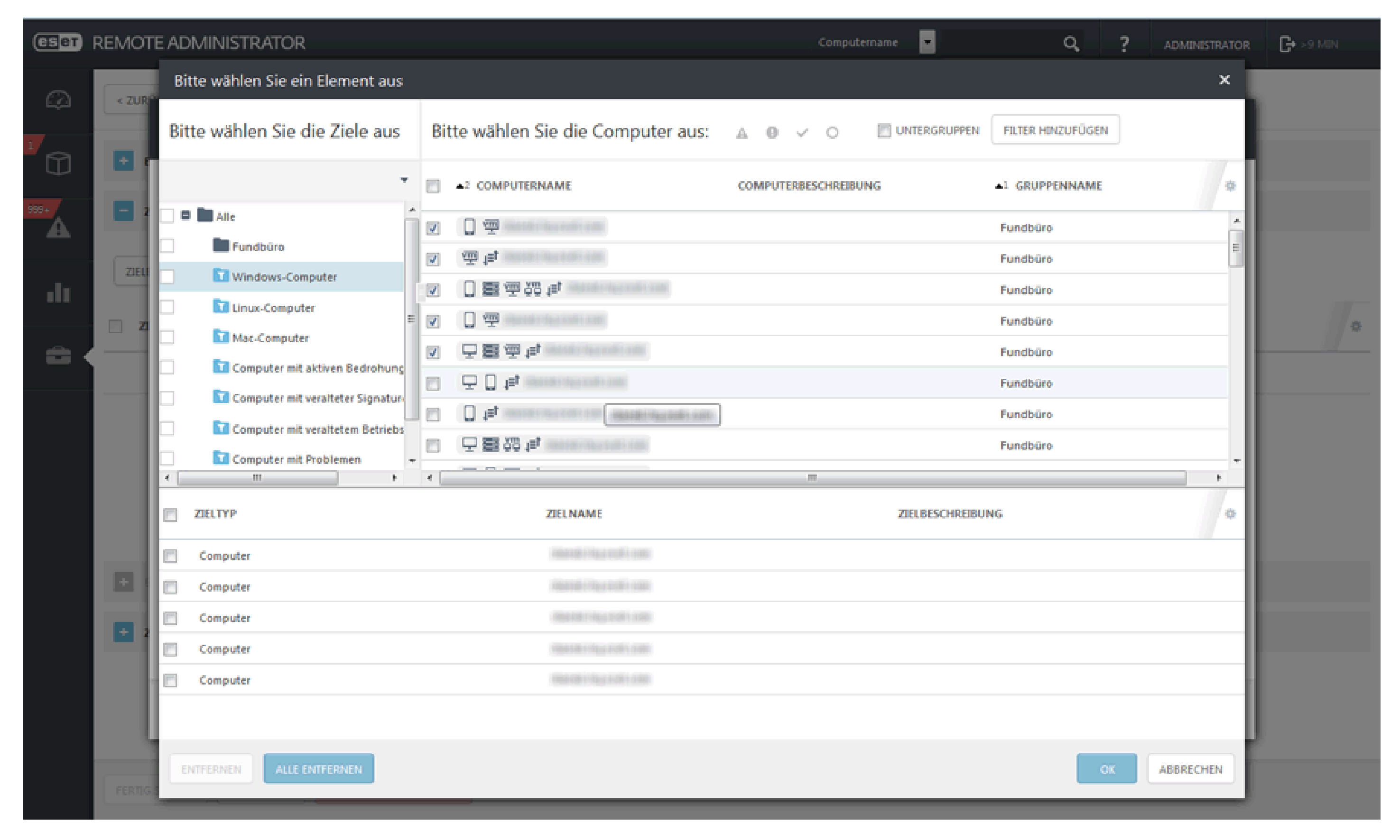
HINWEIS: Für diesen Task sind keine Einstellungen verfügbar.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Zusammenfassung

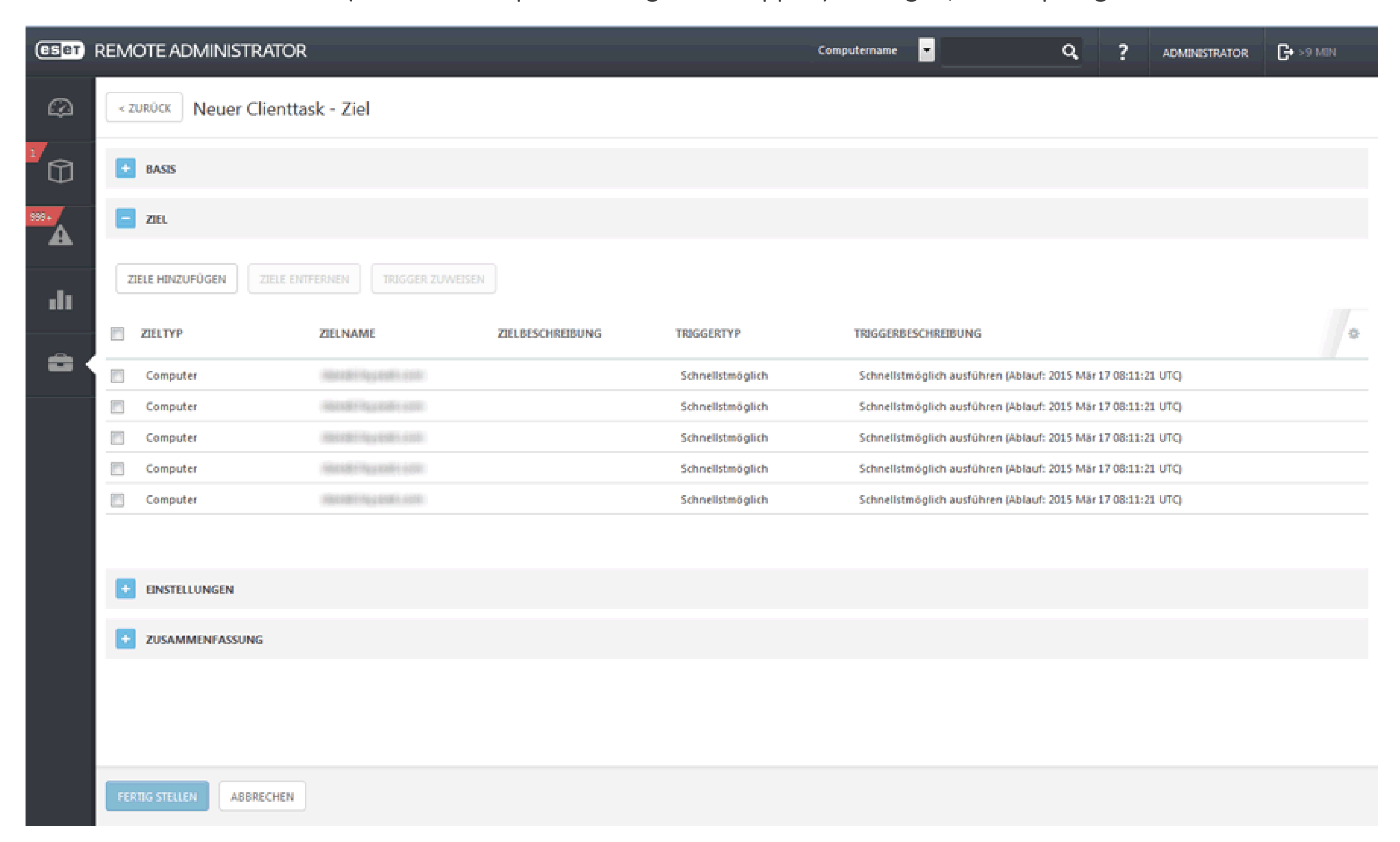
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.5 Upgrade von Remote Administrator-Komponenten

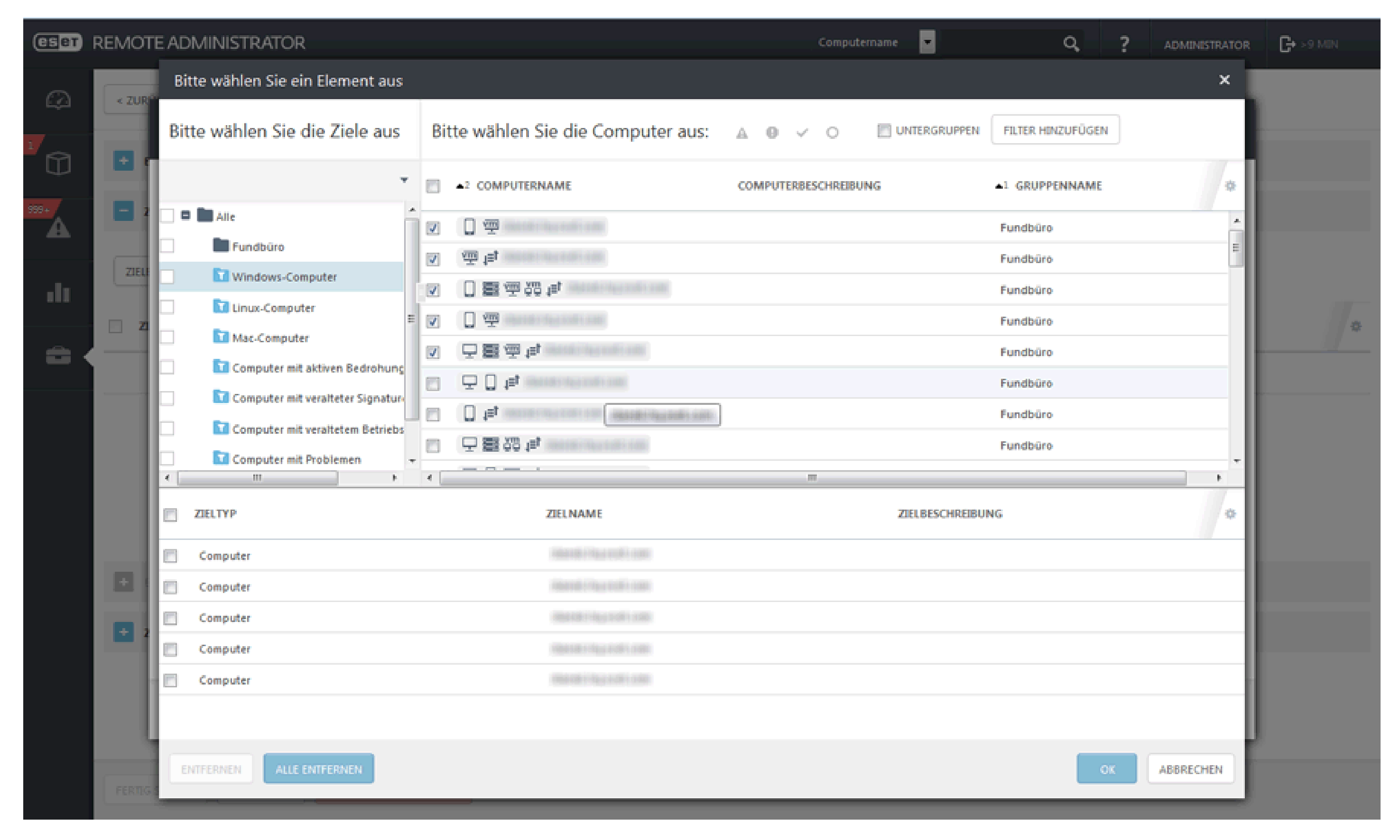
Der Task **Upgrade von Remote Administrator-Komponenten** wird zum Aufrüsten von ERA-Kernkomponenten (Agent, Proxy, Server und MDM) eingesetzt, die auf dem Client installiert sind. Die Aufrüstung erfolgt auf die Version, die mit einem bestimmten ERA-Server (Referenzserver) kompatibel ist.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Remote Administration-Referenzserver** – Wählen Sie aus der Liste die ERA-Serverversion aus. Alle ERA-Komponenten werden auf Versionen aufgerüstet, die mit dem ausgewählten Server kompatibel sind.
- **Bei Bedarf automatisch neu starten** – Mit dieser Option können Sie einen Neustart des Client-Betriebssystems erzwingen, falls dies für die Installation erforderlich ist.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

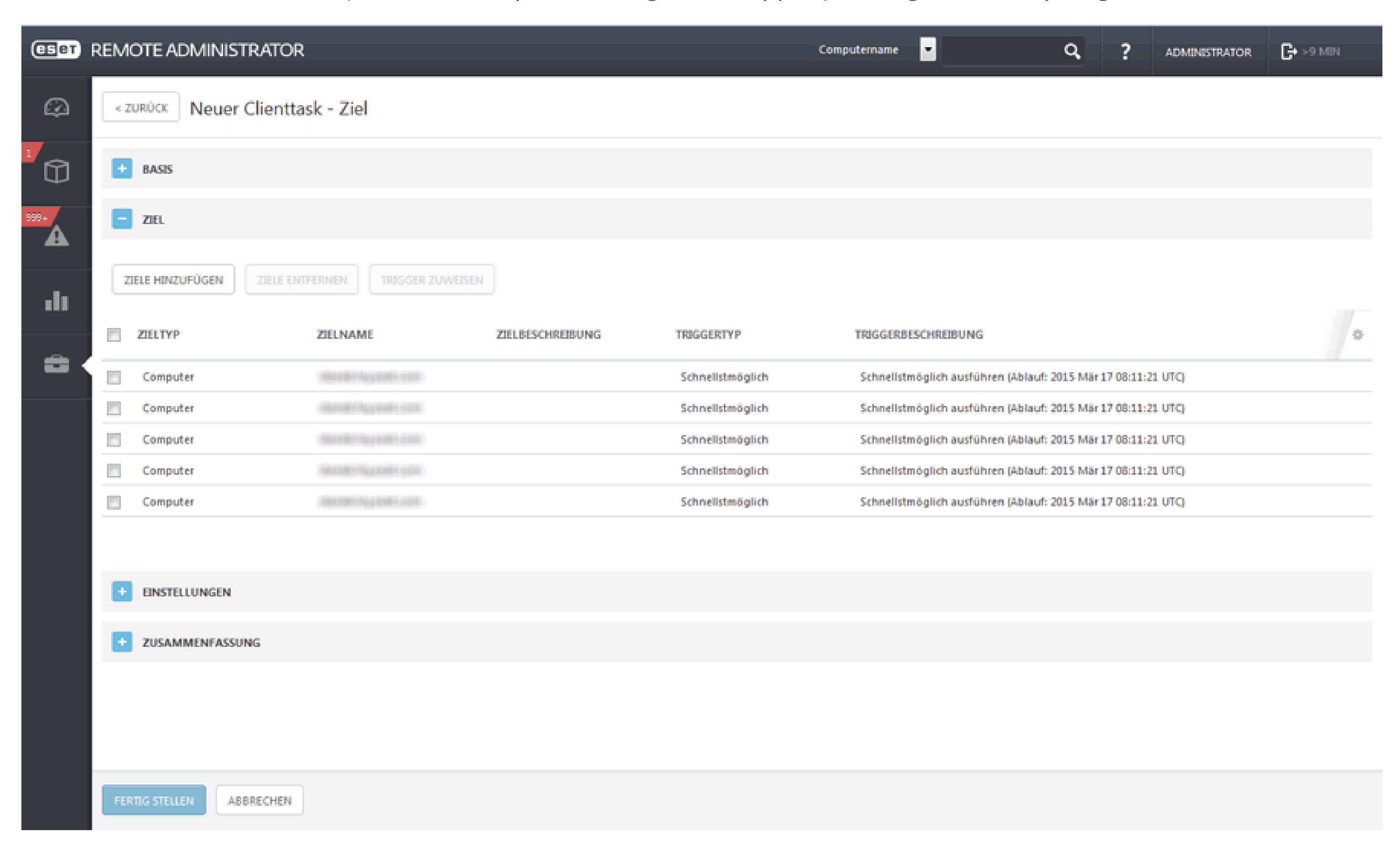
6.1.3.2.6 Geklonten Agenten zurücksetzen

Mit dem Task **Geklonten Agenten zurücksetzen** können Sie den ESET-Agenten im Netzwerk über ein vordefiniertes Image verteilen. Geklonte Agenten haben dieselbe SID. Dies kann Probleme verursachen (mehrere Agenten mit derselben SID). Führen Sie in diesem Fall den Task „Geklonten Agenten zurücksetzen“ aus, um die SID zurückzusetzen und den Agenten eine eindeutige Identität zuzuweisen.

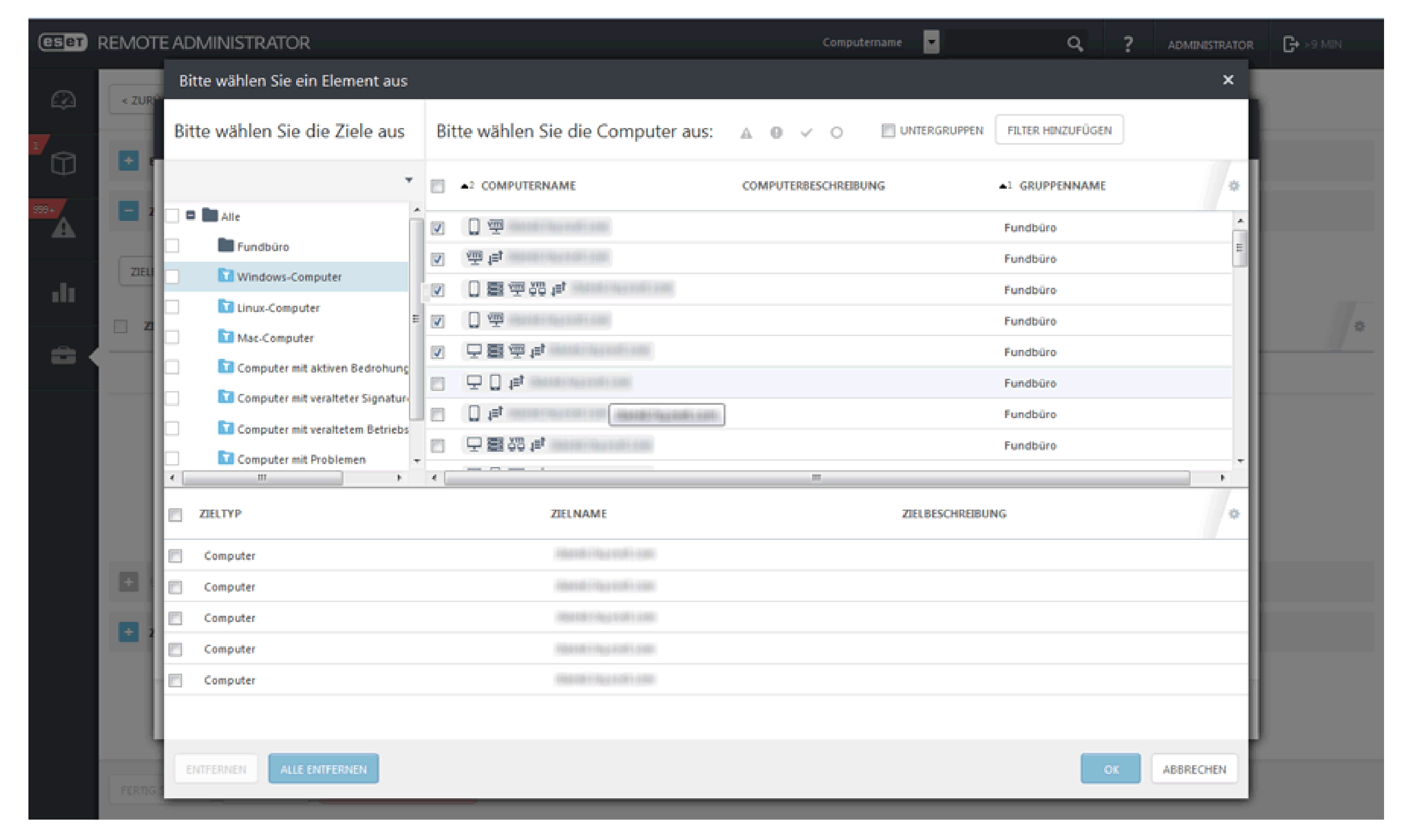
HINWEIS: Für diesen Task sind keine Einstellungen verfügbar.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Zusammenfassung

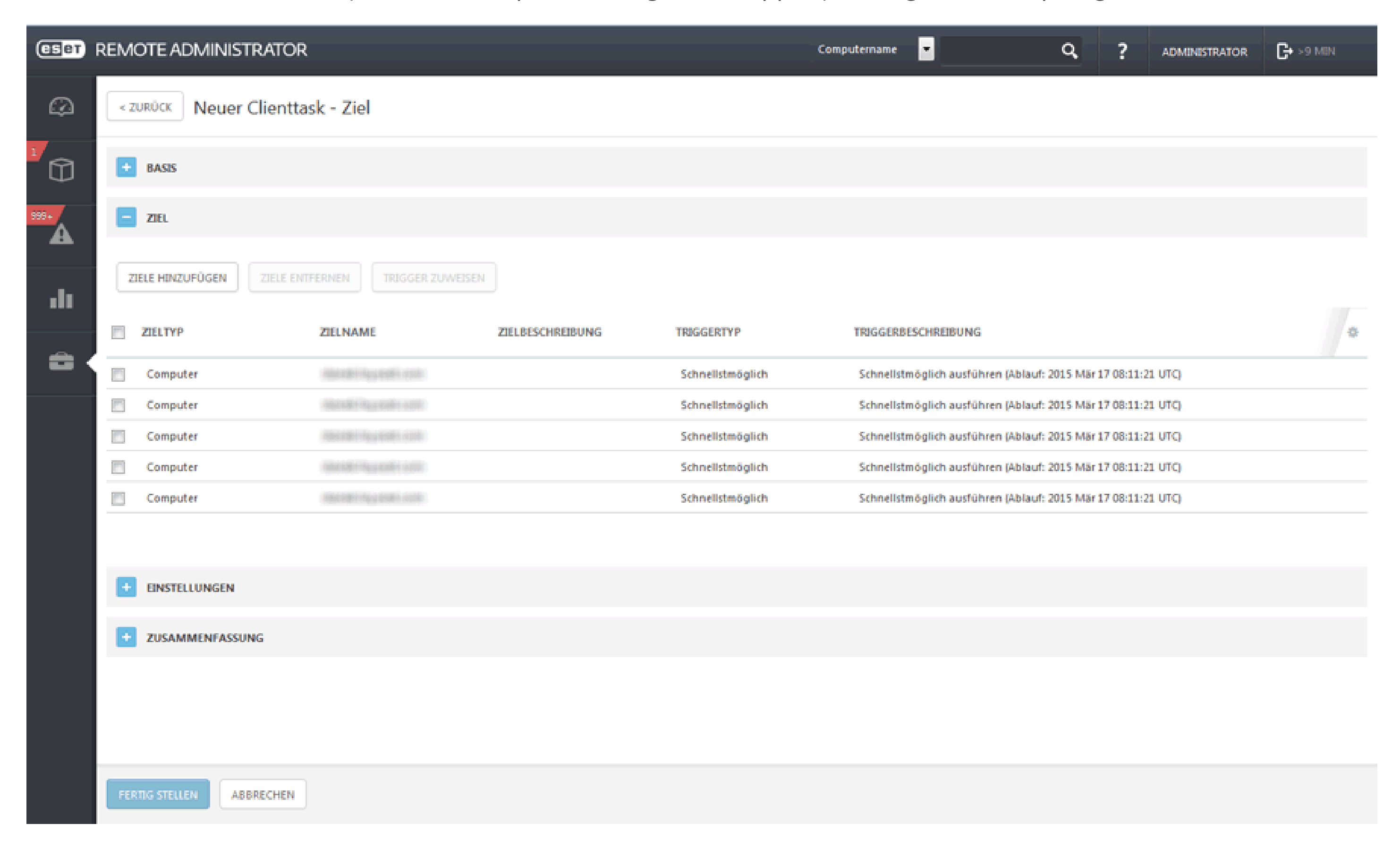
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.7 Befehl ausführen

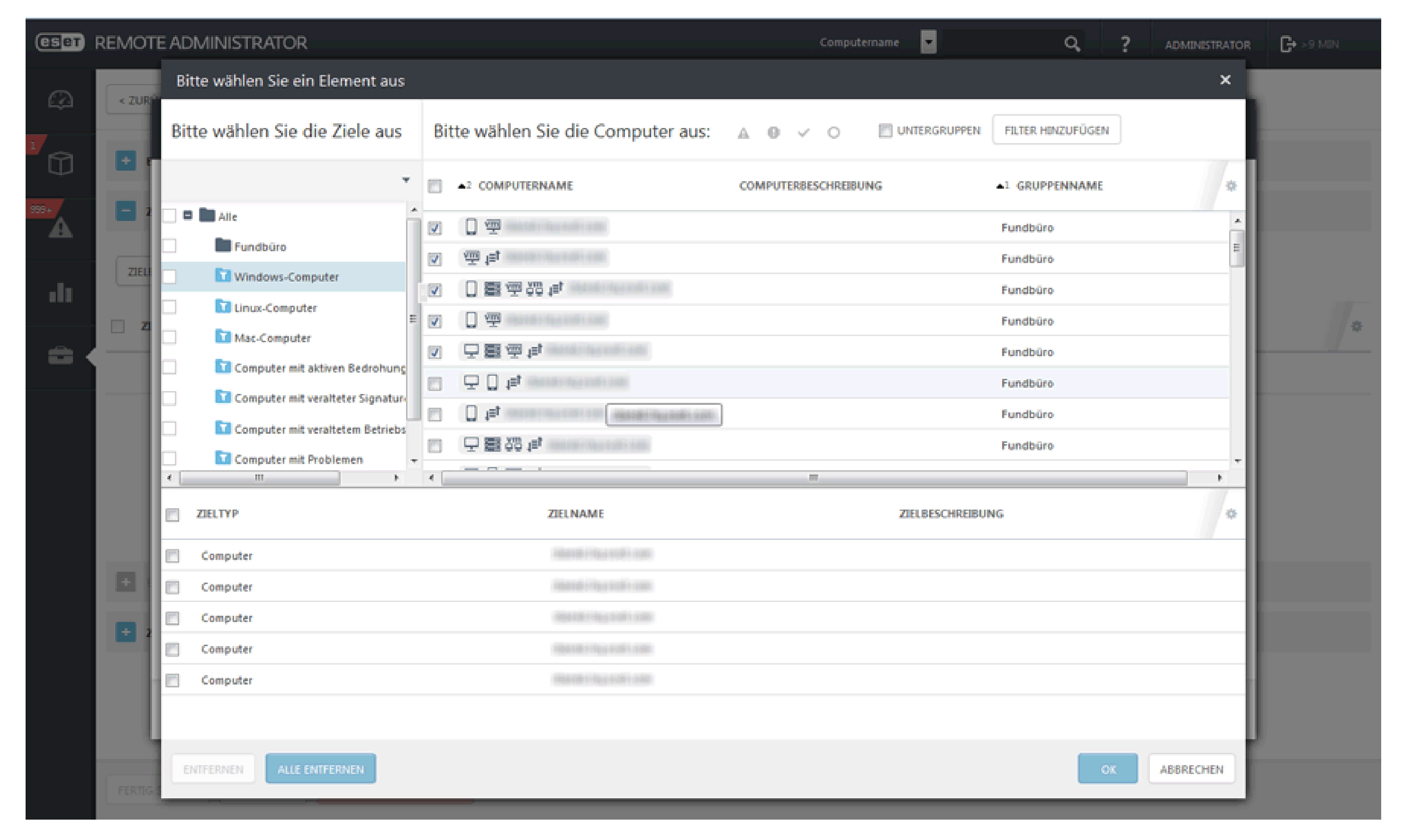
Mit dem Task **Befehl ausführen** können Sie spezielle Befehlszeilenanweisungen auf dem Client ausführen. Der Administrator legt die auszuführende Befehlszeile fest.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Auszuführende Befehlszeile** – Geben Sie die Befehlszeile ein, die auf dem/den Client(s) ausgeführt werden soll.
- **Arbeitsverzeichnis** – Geben Sie das Verzeichnis ein, in dem die oben festgelegte Befehlszeile ausgeführt werden soll.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen", wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

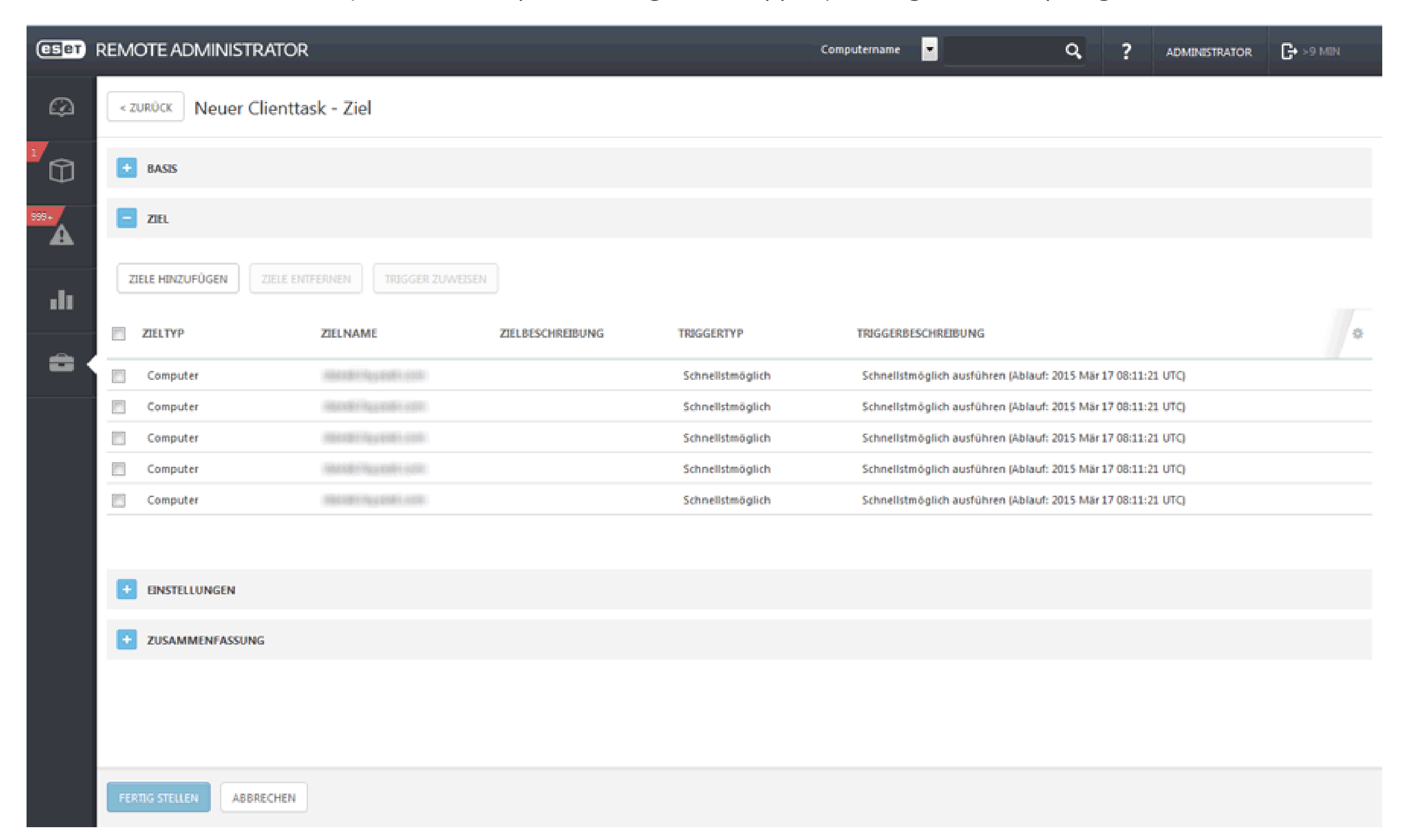
6.1.3.2.8 SysInspector-Skript ausführen

Mit dem Task **SysInspector-Skript ausführen** können Sie unerwünschte Objekte aus dem System entfernen. Vor dem Ausführen dieses Tasks muss ein **SysInspector-Skript** von ESET-SysInspector exportiert werden. Nachdem Sie das Skript exportiert haben, können Sie die zu entfernenden Objekte markieren und das Skript mit den geänderten Daten ausführen. Die markierten Objekte werden gelöscht.

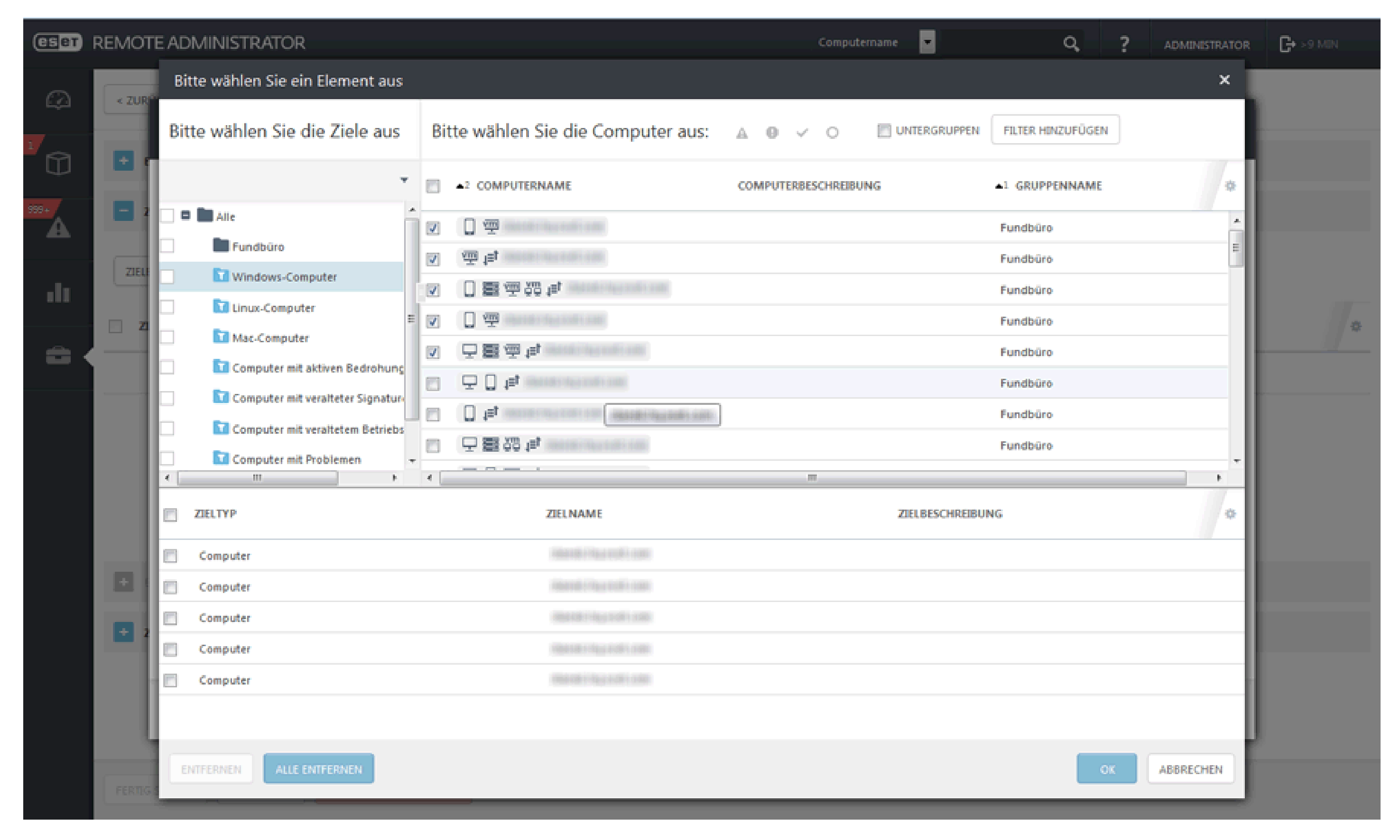
HINWEIS: Nach dem Abschluss des Tasks können Sie die Ergebnisse in einem Bericht überprüfen.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **SysInspector-Skript** – Klicken Sie auf **Durchsuchen**, um das Skript auszuwählen. Das Dienstskript muss vor dem Ausführen des Tasks erstellt werden.
- **Aktion** – Wählen Sie **Upload** oder **Download** aus, um ein Skript in die ERA-Konsole hochzuladen oder von dort herunterzuladen.

Zusammenfassung

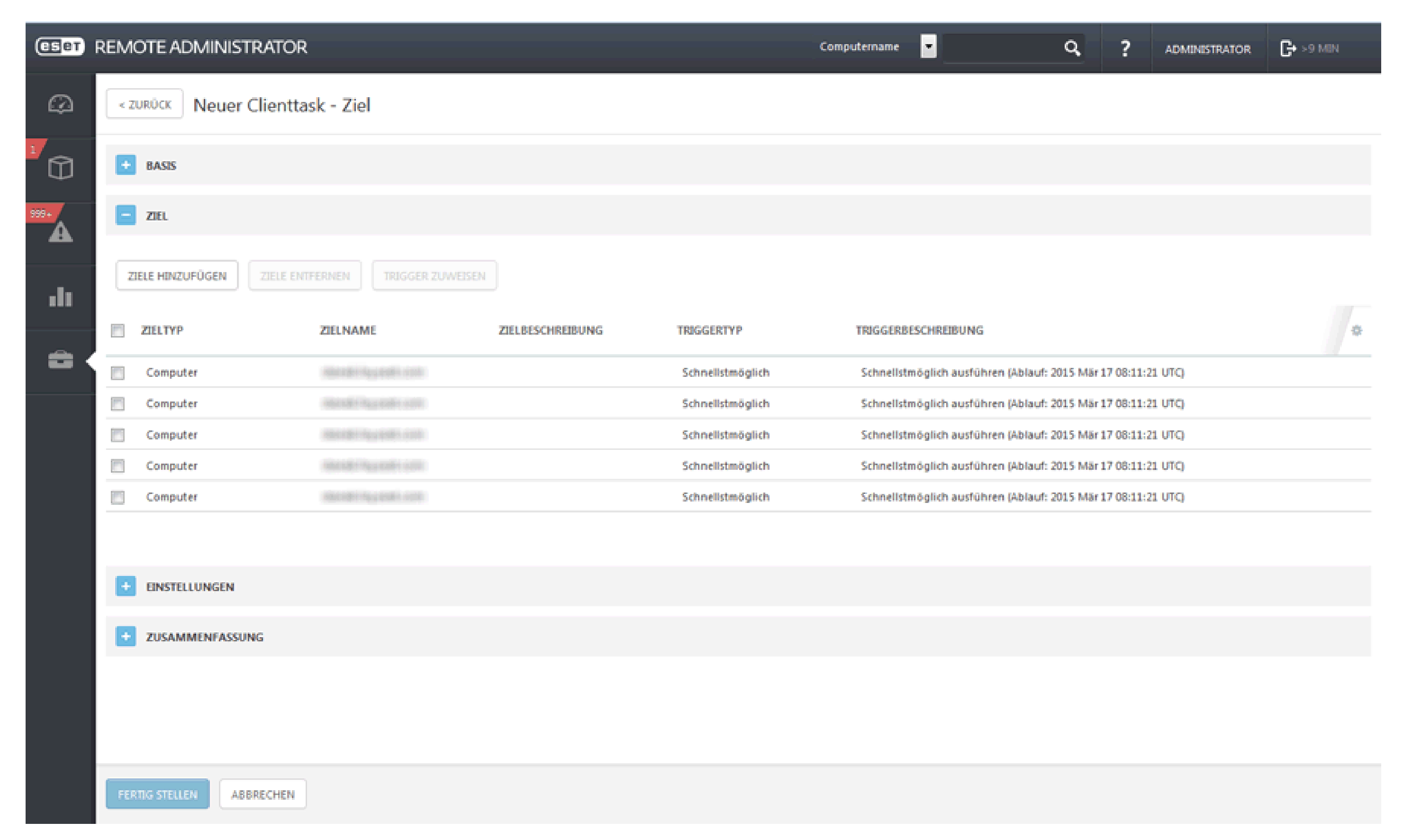
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.9 Software-Installation

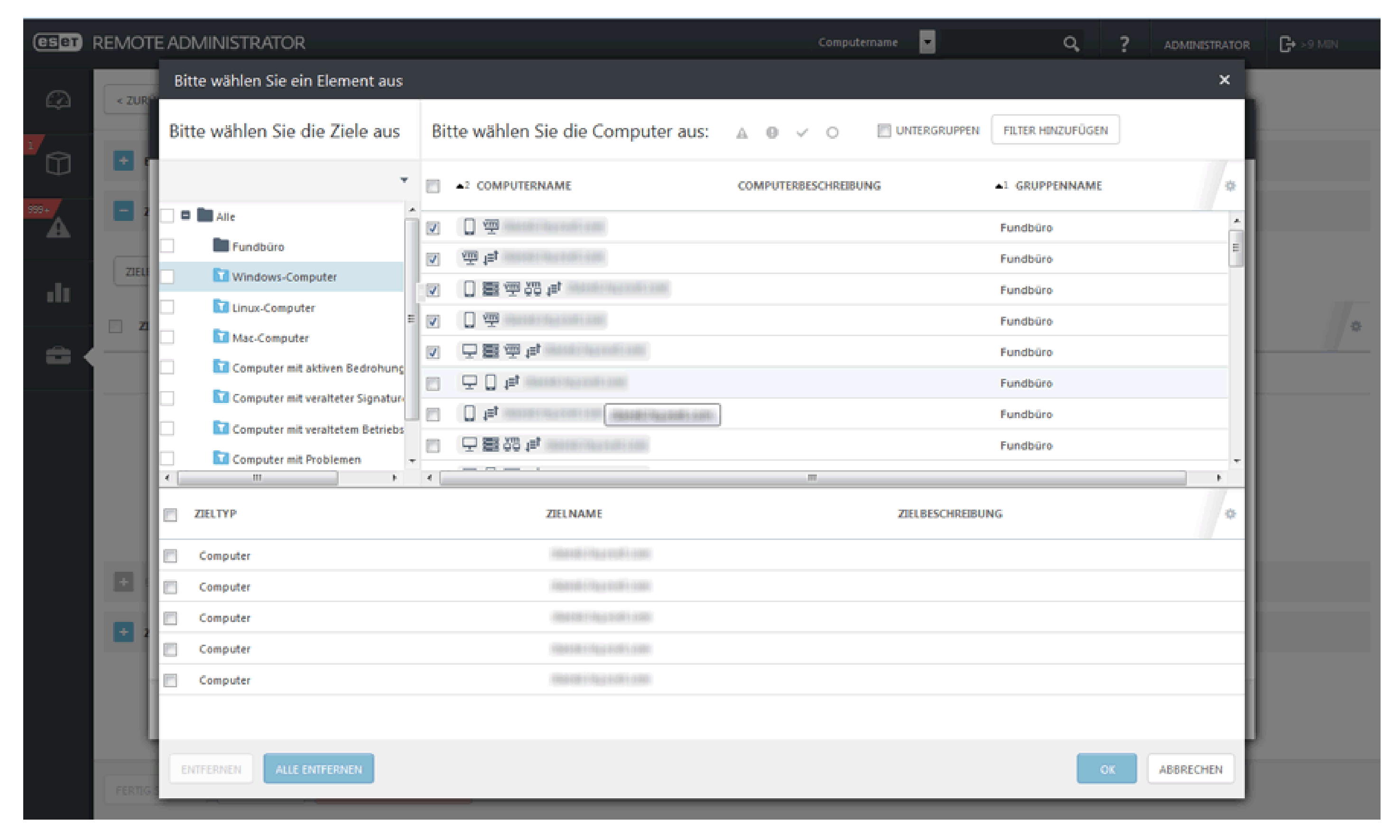
Mit dem Task **Software-Installation** installieren Sie Software auf den Clientcomputern. Der Task wurde hauptsächlich für die Installation von ESET-Produkten entwickelt, kann jedoch zur Installation beliebiger anderer Software verwendet werden. Führen Sie die folgenden Anweisungen aus oder sehen Sie sich das Anleitungsvideo in der Knowledgebase an.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Klicken Sie auf **<ESET-Lizenz auswählen>** und wählen Sie aus der Liste der verfügbaren Lizenzen die geeignete Lizenz für das installierte Produkt aus. Aktivieren Sie das Kontrollkästchen neben **Ich stimme der Endbenutzer-Lizenzvereinbarung für die Anwendung zu**, sofern Sie zustimmen. Weitere Informationen hierzu finden Sie unter Lizenzverwaltung oder EULA.

Klicken Sie auf **<Paket auswählen>**, um ein Installationspaket aus dem Repository auszuwählen, oder geben Sie eine Paket-URL ein. Eine Liste verfügbarer Pakete wird angezeigt, in der Sie das zu installierende ESET-Produkt (zum Beispiel ESET Endpoint Security) auswählen können. Wählen Sie das gewünschte Installationspaket aus und klicken Sie auf **OK**. Wenn Sie eine URL für das Installationspaket angeben möchten, geben Sie die URL durch Eintippen oder Kopieren und Einfügen in das Textfeld ein (verwenden Sie keine URLs, die Authentifizierung erfordern).

HINWEIS: Beachten Sie, dass Server und Agent mit dem Internet verbunden sein müssen, um auf das Repository zugreifen und die Installation durchführen zu können. Falls Sie keinen Internetzugriff haben, können Sie die Clientsoftware lokal installieren.

Bei Bedarf können Sie Installationsparameter angeben. Andernfalls lassen Sie dieses Feld leer. Aktivieren Sie das Kontrollkästchen neben Bei Bedarf automatisch neu starten, um einen automatischen Neustart des Computers nach der Installation zu erzwingen. Sie können diese Option auch deaktiviert lassen. Die Entscheidung über den Neustart wird dann vom Benutzer des Clientcomputers getroffen.

Zusammenfassung

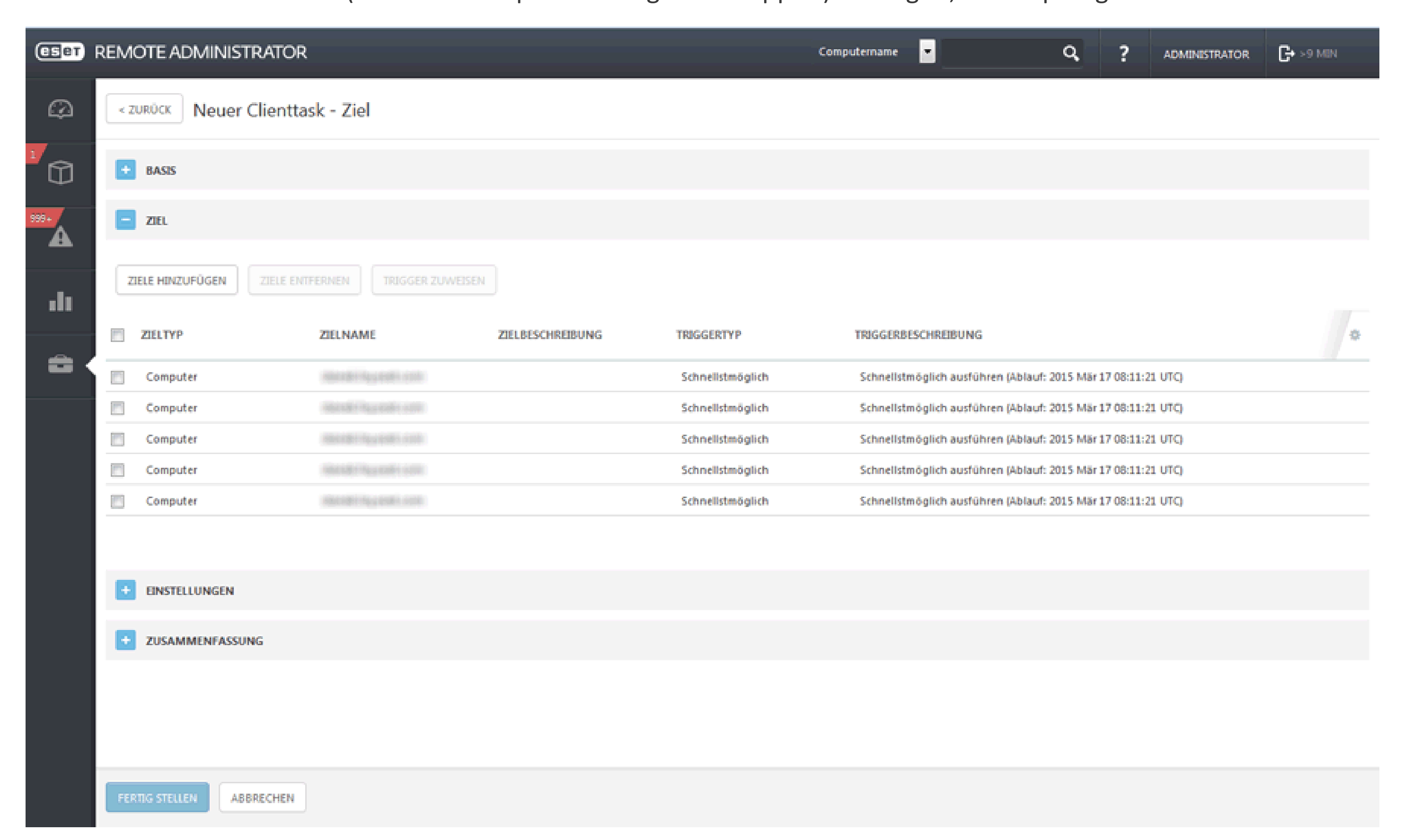
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen", wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.10 Software-Deinstallation

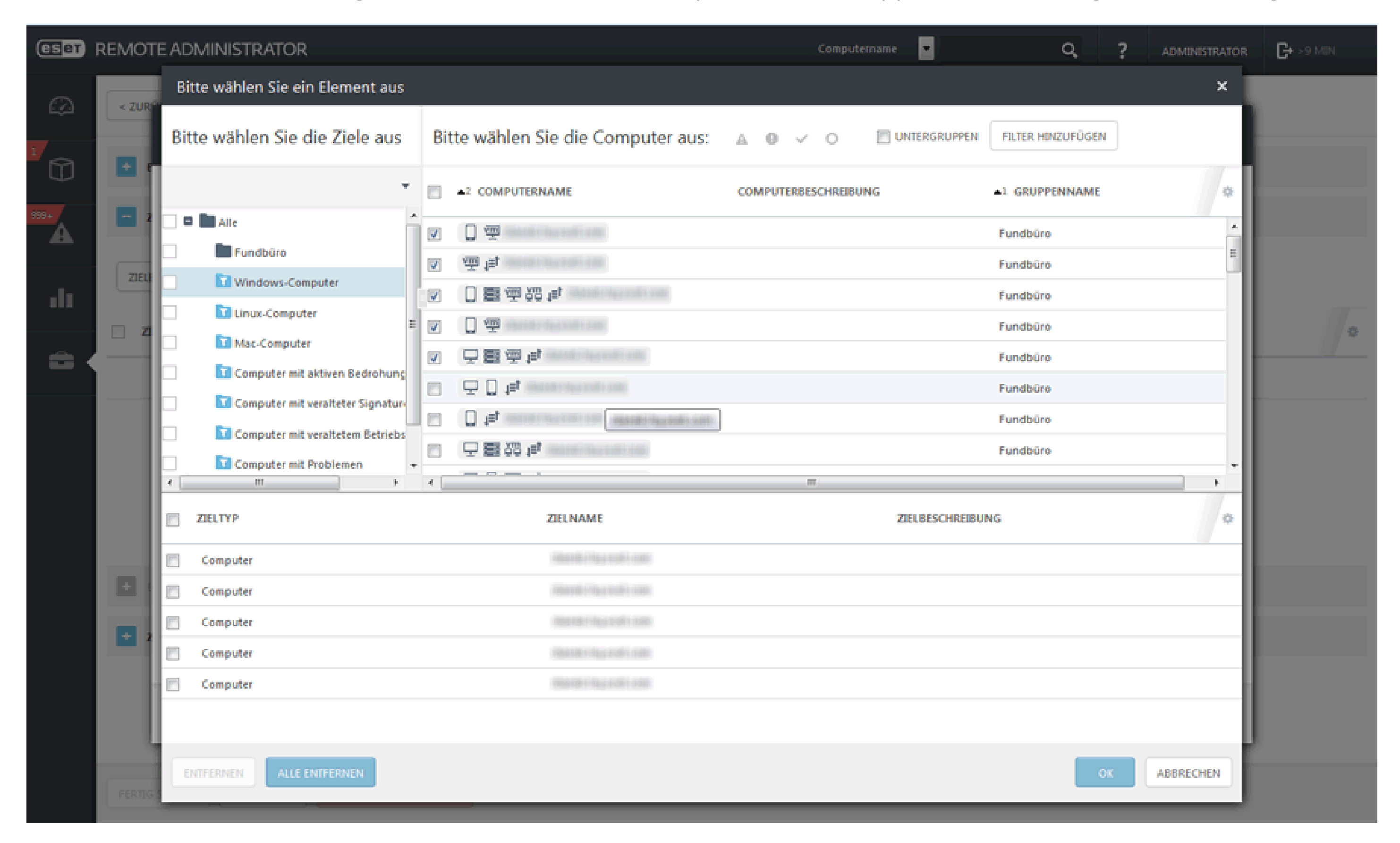
Mit dem Task **Software-Deinstallation** können Sie ESET-Produkte von den Clients deinstallieren, wenn Sie nicht mehr erwünscht sind oder nicht mehr benötigt werden. Wenn Sie den ERA-Agenten deinstallieren, werden in den ESET-Produkten, die von diesem Agenten verwaltet wurden, nach der Deinstallation des Agenten möglicherweise einige Einstellungen beibehalten.
Es empfiehlt sich, bestimmte Einstellungen (z. B. für den Passwortschutz) mithilfe einer Policy auf den Standardwert zurückzusetzen, bevor das Gerät von der Verwaltung ausgeschlossen wird. Außerdem werden alle auf dem Agenten ausgeführten Tasks abgebrochen. Der Ausführungsstatus **Wird ausgeführt**, **Fertig** oder **Fehler des Tasks** wird je nach Replikation möglicherweise nicht richtig in der ERA Web-Konsole angezeigt.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Einstellungen für Software-Deinstallation

- **Deinstallieren** - **Anwendung aus der Liste:**

Paketname – Wählen Sie eine ERA-Komponente oder ein Client-Sicherheitsprodukt aus. In dieser Liste werden alle Pakete angezeigt, die auf den ausgewählten Clients installiert sind.
Paketversion – Sie können entweder eine bestimmte Version des Pakets (beispielsweise wenn eine bestimmte Paketversion Probleme verursacht) oder alle Versionen des Pakets entfernen.
Bei Bedarf automatisch neu starten – Mit dieser Option können Sie einen Neustart des Client-Betriebssystems erzwingen, falls dies für die Deinstallation erforderlich ist.

- **Uninstall** - **Virenschutz-Software eines Drittanbieters (erstellt mit OPSWAT) -** Eine Liste kompatibler Virenschutzsoftware finden Sie in unserem KnowledgeBase-Artikel. Dieser Vorgang unterscheidet sich von der Deinstallation via **Programme hinzufügen oder entfernen**. Er verwendet alternative Methoden zur Entfernung externer Antivirensoftware und löscht sorgfältig alle verbleibenden Registrierungseinträge und sonstige Spuren.

Führen Sie die schrittweisen Anweisungen in diesem Artikel aus: Entfernen von Virenschutz-Software eines Drittanbieters von Clientcomputern mithilfe von ESET Remote Administrator (6.x) um einen Task zur Entfernung externer Antivirensoftware an Clientcomputer senden.

Zusammenfassung

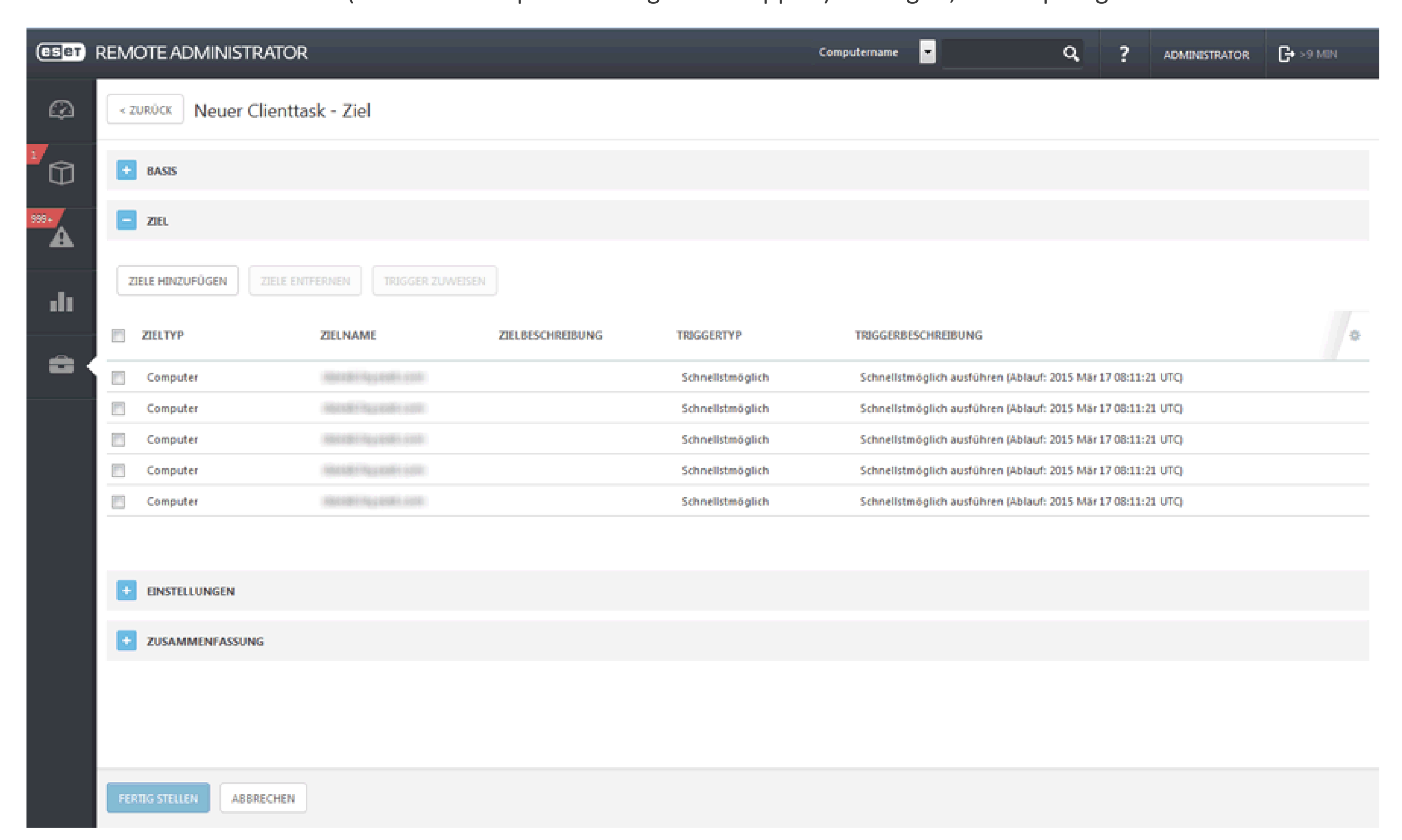
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.11 Produktaktivierung

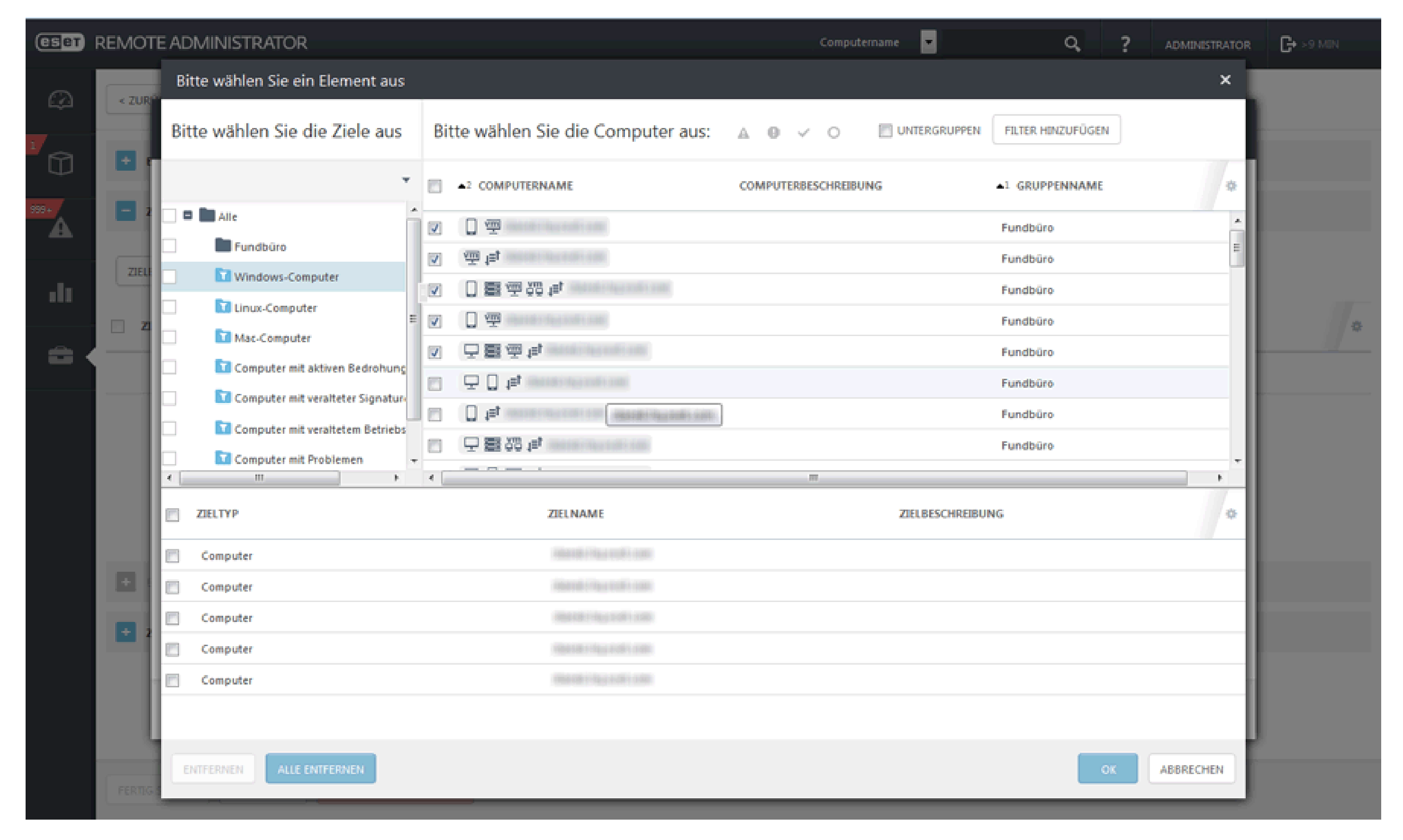
Befolgen Sie diese Schritte, um ein ESET-Produkt auf einem Clientcomputer zu aktivieren:

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Produktaktivierungseinstellungen - Wählen Sie in der Liste eine Lizenz für den Client aus. Die Lizenz wird auf die bereits auf dem Client installierten Produkte angewendet.

Zusammenfassung

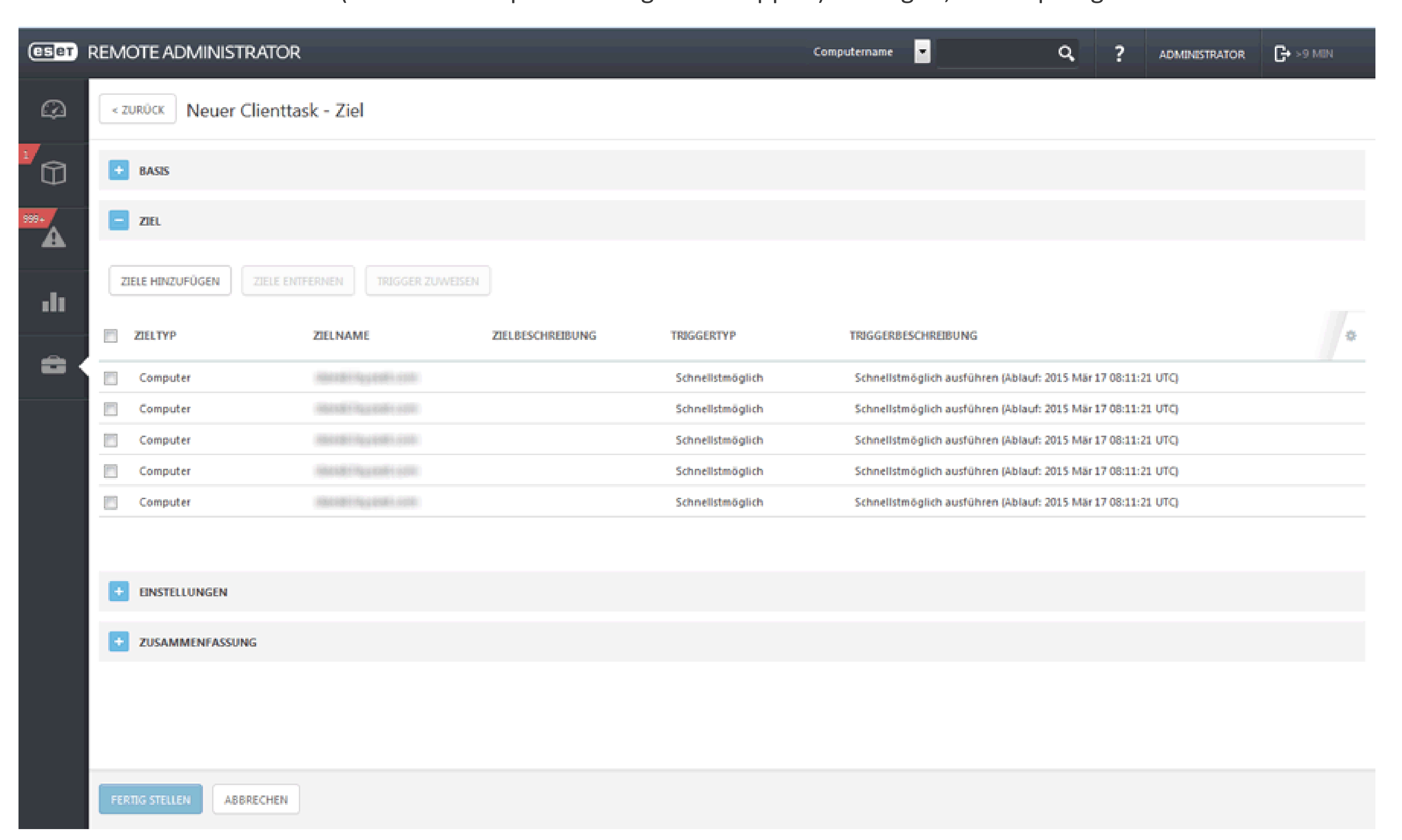
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.12 SysInspector-Loganfrage

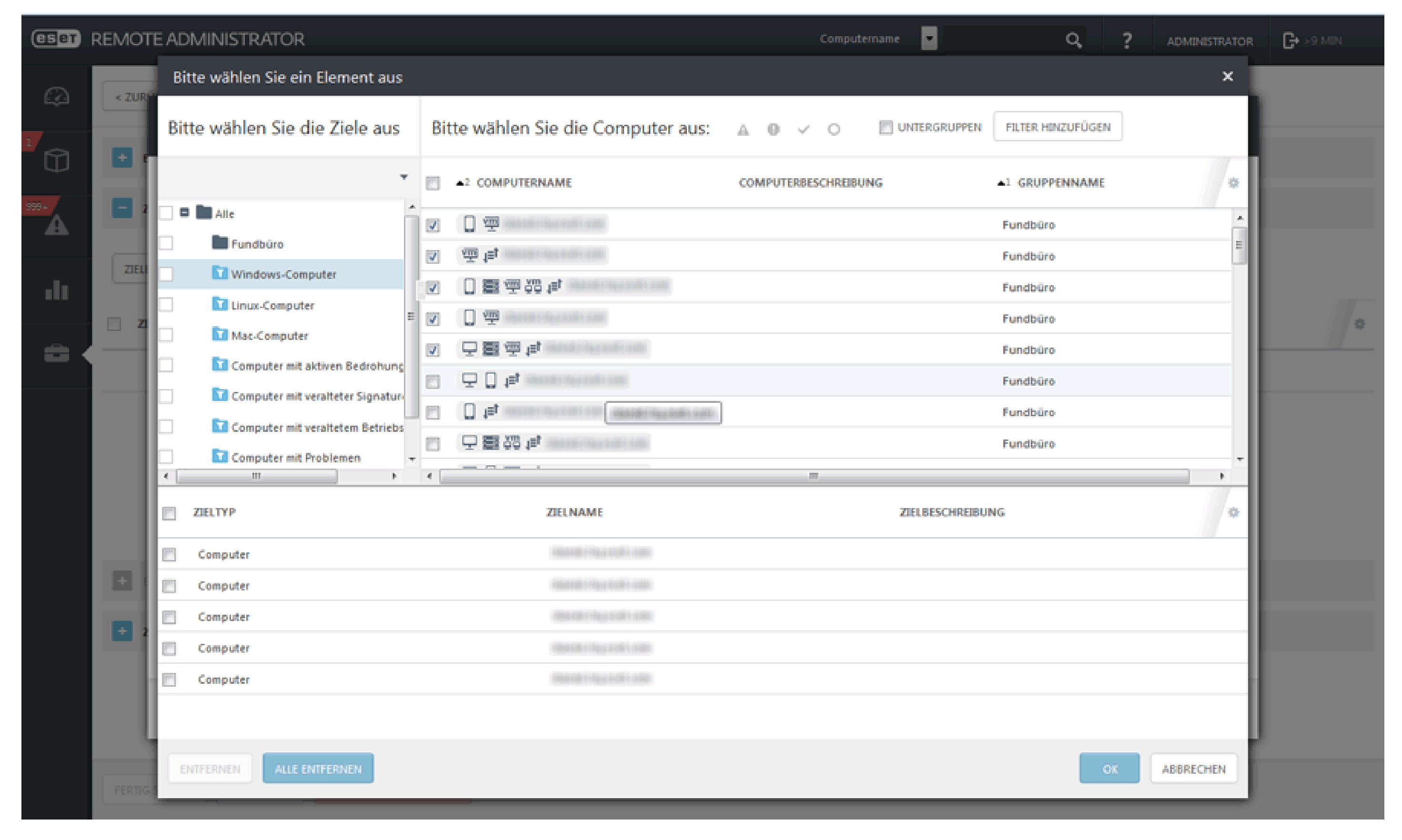
Mit dem Task **SysInspector-Loganfrage** wird der SysInspector-Log eines Client-Sicherheitsprodukts angefordert, das über diese Funktion verfügt.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Log auf Client speichern** – Wählen Sie diese Option aus, wenn der SysInspector-Log auf dem Client und auf dem ERA-Server gespeichert werden soll. Auf einem Client mit ESET Endpoint Security wird der Log zum Beispiel üblicherweise unter *C:\Program Data\ESET\ESET Endpoint Antivirus\SysInspector* gespeichert.

- **Vergleich zum letzten Snapshot vor einem bestimmten Zeitpunkt** – Mit dieser Option können Sie den erzeugten Log mit Logs aus einem bestimmten früheren Zeitraum vergleichen. Mithilfe der Vergleichsinformationen können Sie Unterschiede und Änderungen auf dem Client ermitteln.

Zusammenfassung

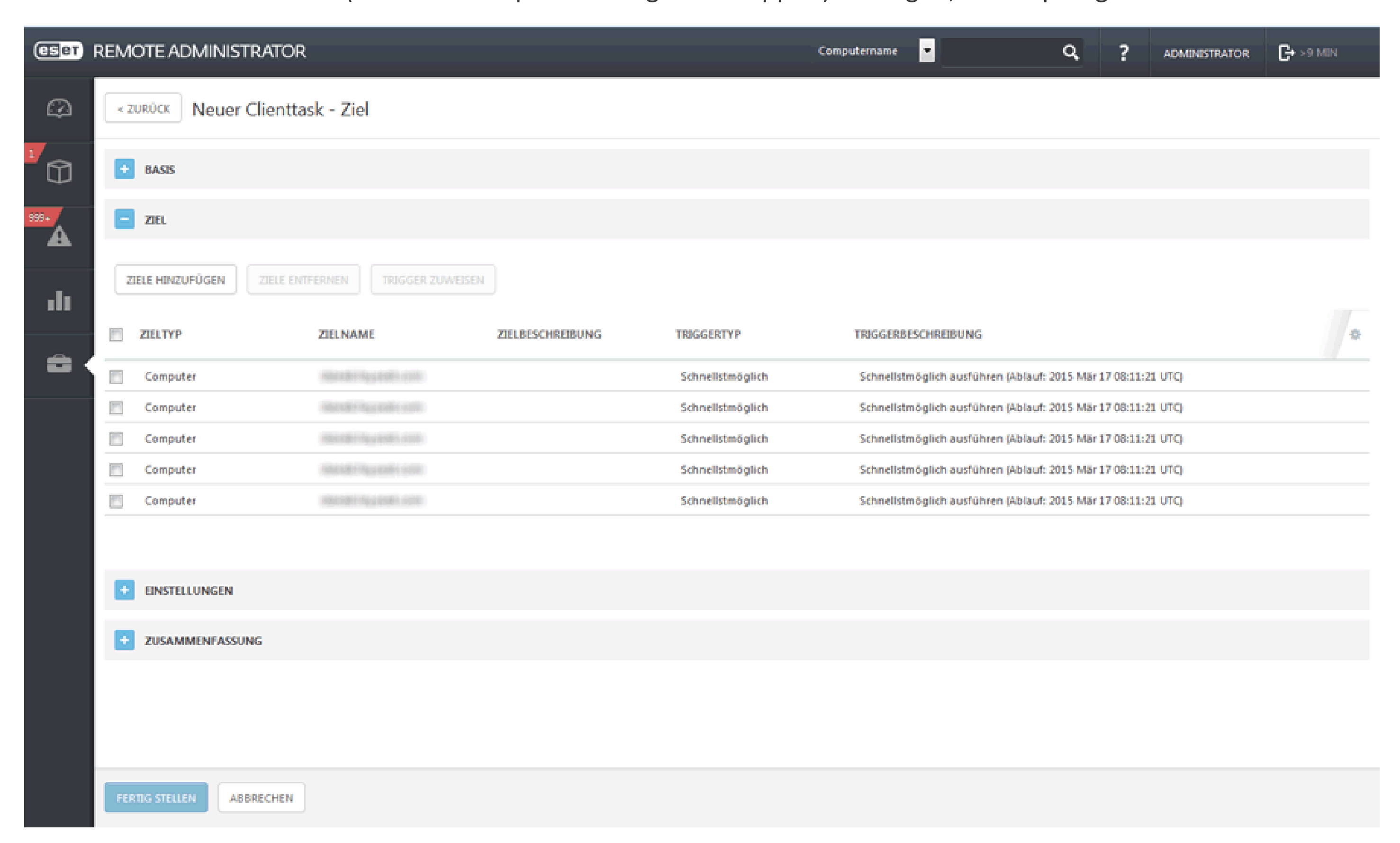
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.13 Quarantänedatei hochladen

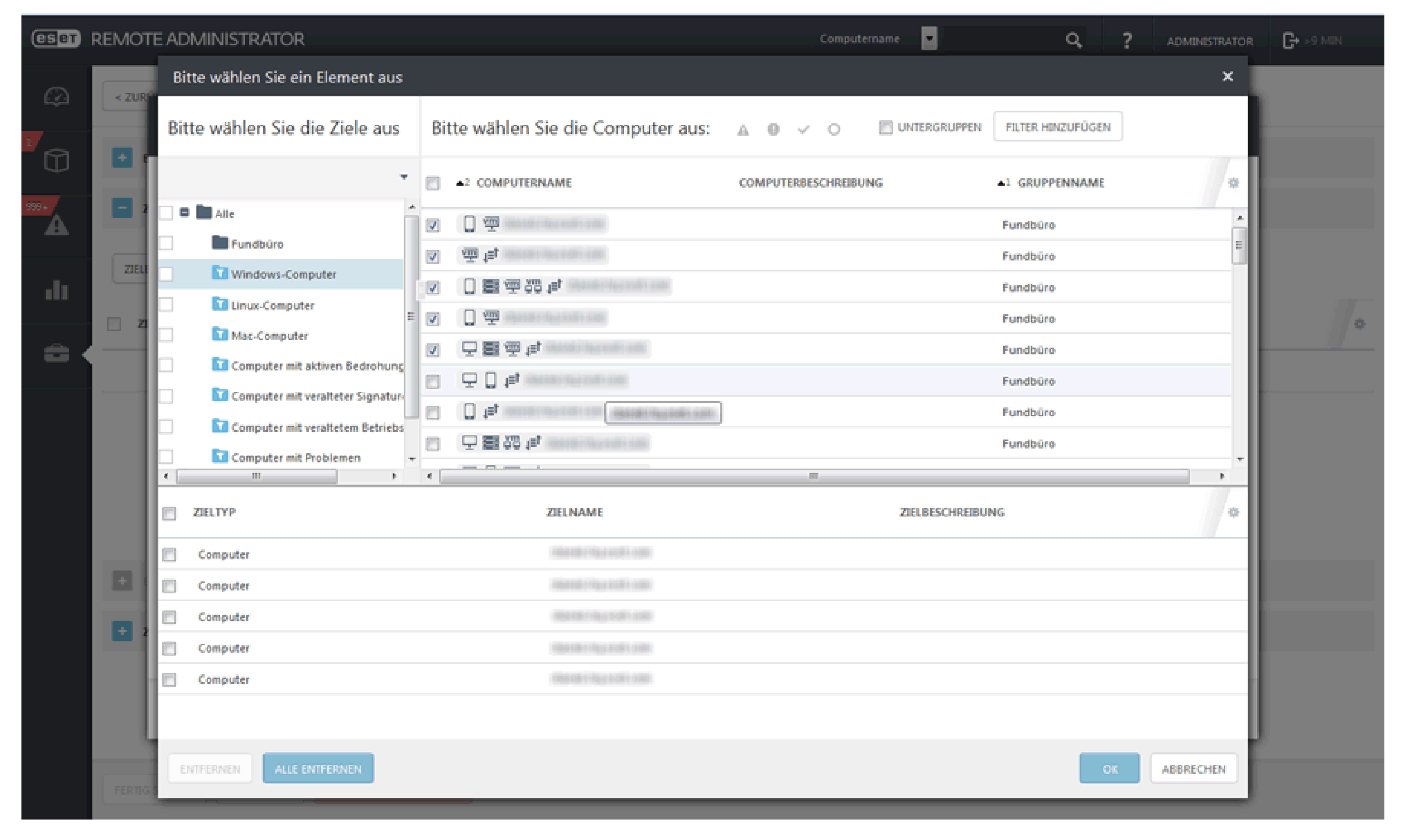
Mit dem Task **Quarantänedatei hochladen** können Sie Dateien verwalten, die auf den Clients in die Quarantäne verschoben wurden.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Objekt in Quarantäne** – Wählen Sie ein Objekt aus der Quarantäne aus.
- **Objektpasswort** – Geben Sie ein Passwort zum Verschlüsseln des Objekts ein. Beachten Sie, dass das Passwort im entsprechenden Bericht angezeigt wird.
- **Upload-Pfad** – Geben Sie den Pfad zu einem Speicherort an, zu dem das Objekt hochgeladen werden soll.
- **Benutzername/Passwort für Upload** – Falls für den Speicherort eine Authentifizierung erforderlich ist (Netzwerkfreigabe usw.), geben Sie den Berechtigungsnachweis für diesen Pfad ein.

Zusammenfassung

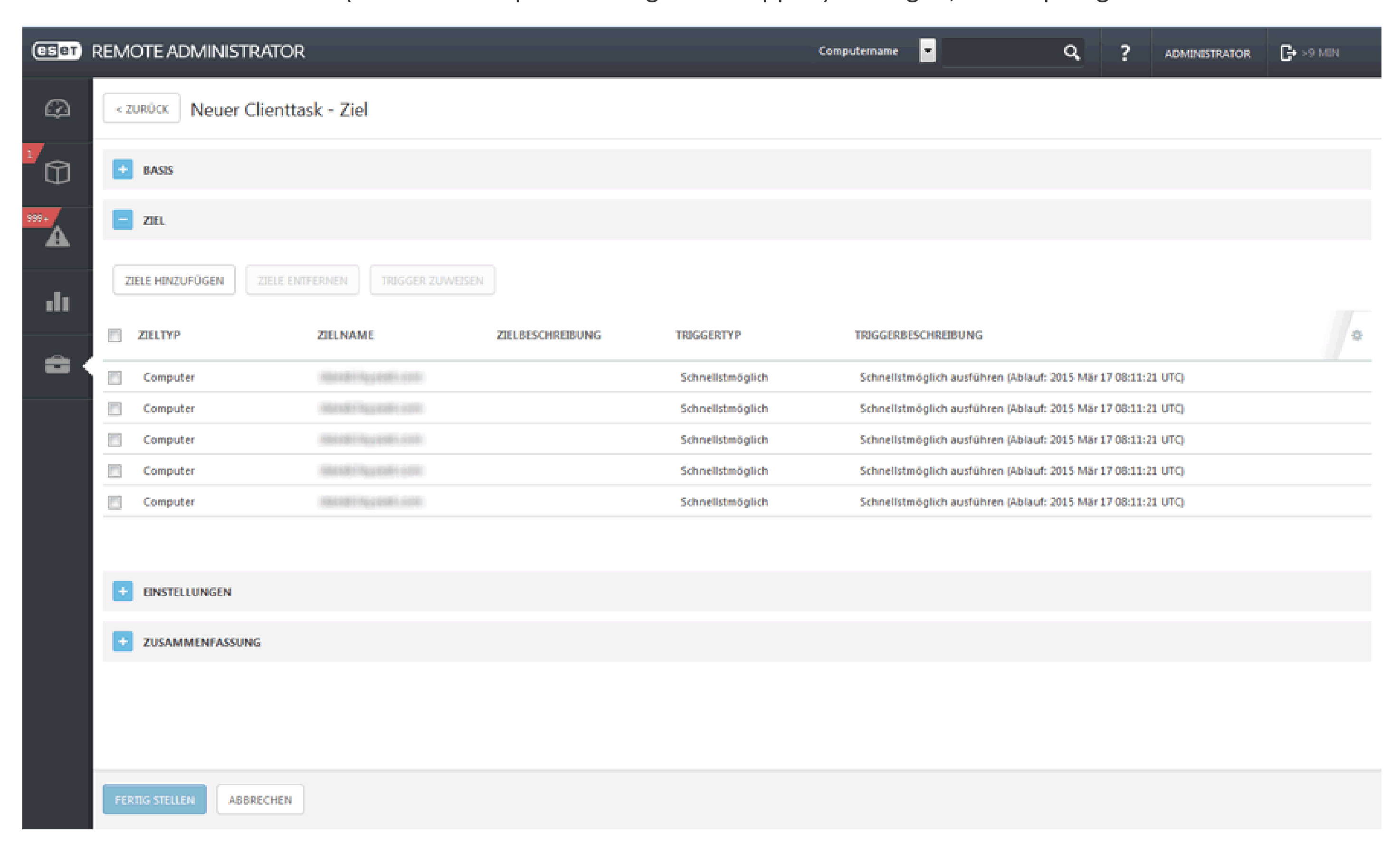
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.14 Update der Signaturdatenbank

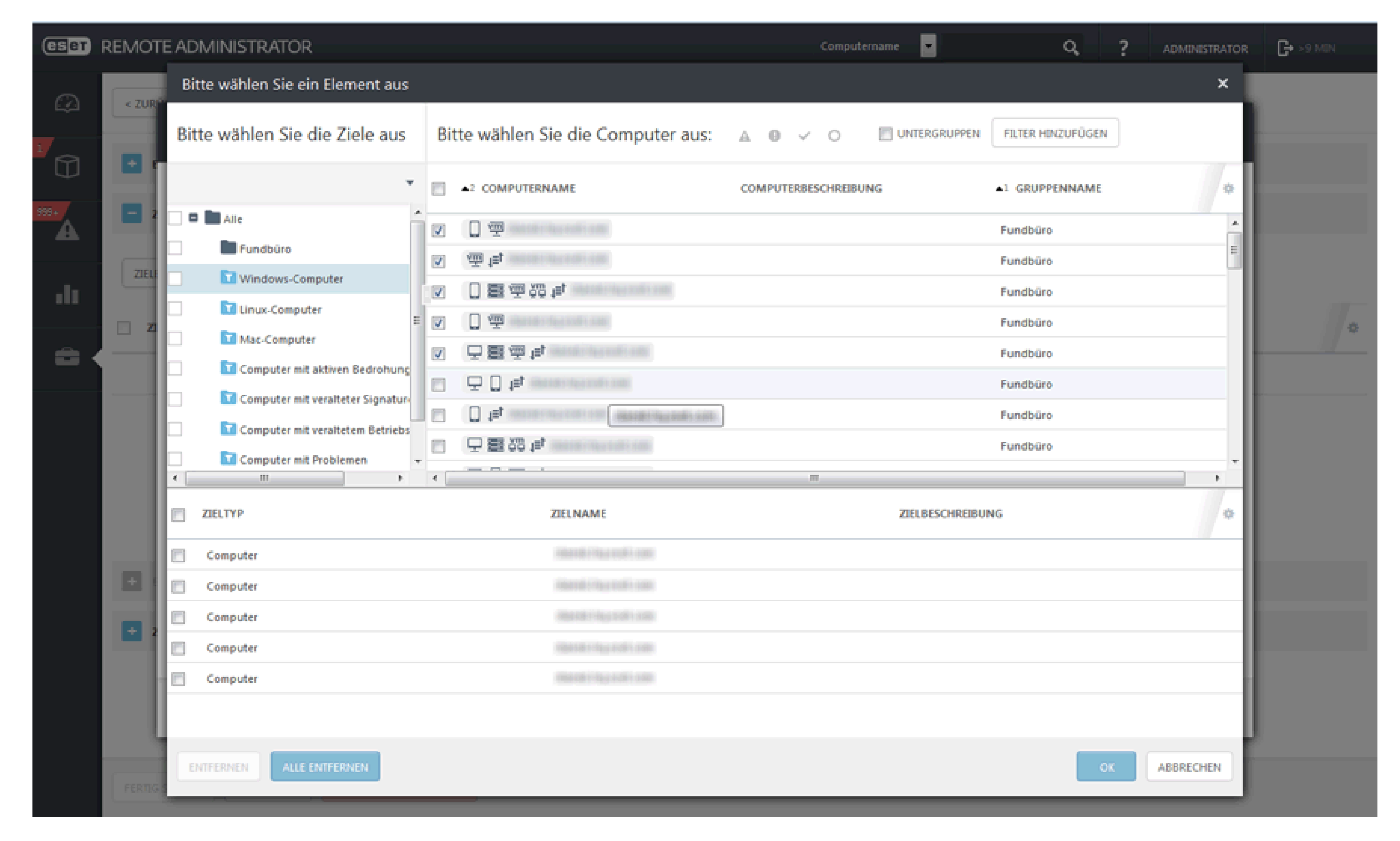
Der Task **Produkt-Update** erzwingt ein Update der Signaturdatenbank des auf den Clients installierten Sicherheitsprodukts. Dies ist ein allgemeiner Task für alle Produkte im System.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Update-Cache löschen** – Mit dieser Option werden die temporären Update-Dateien im Cache auf dem Client gelöscht. Der Task kann hilfreich sein, um Probleme nach einem nicht erfolgreichen Update der Signaturdatenbank zu beheben.

Zusammenfassung

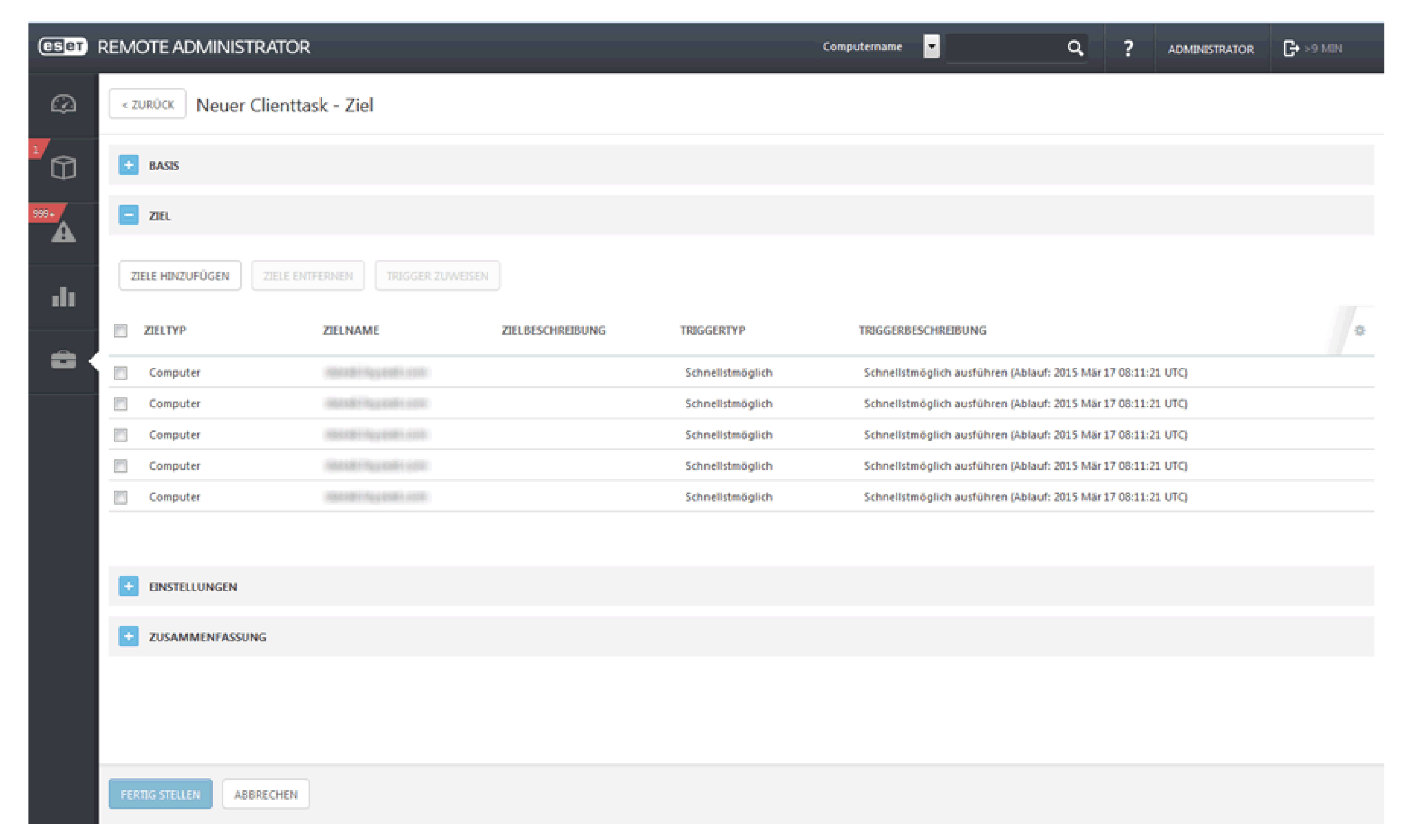
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.15 Rollback eines Updates der Signaturdatenbank

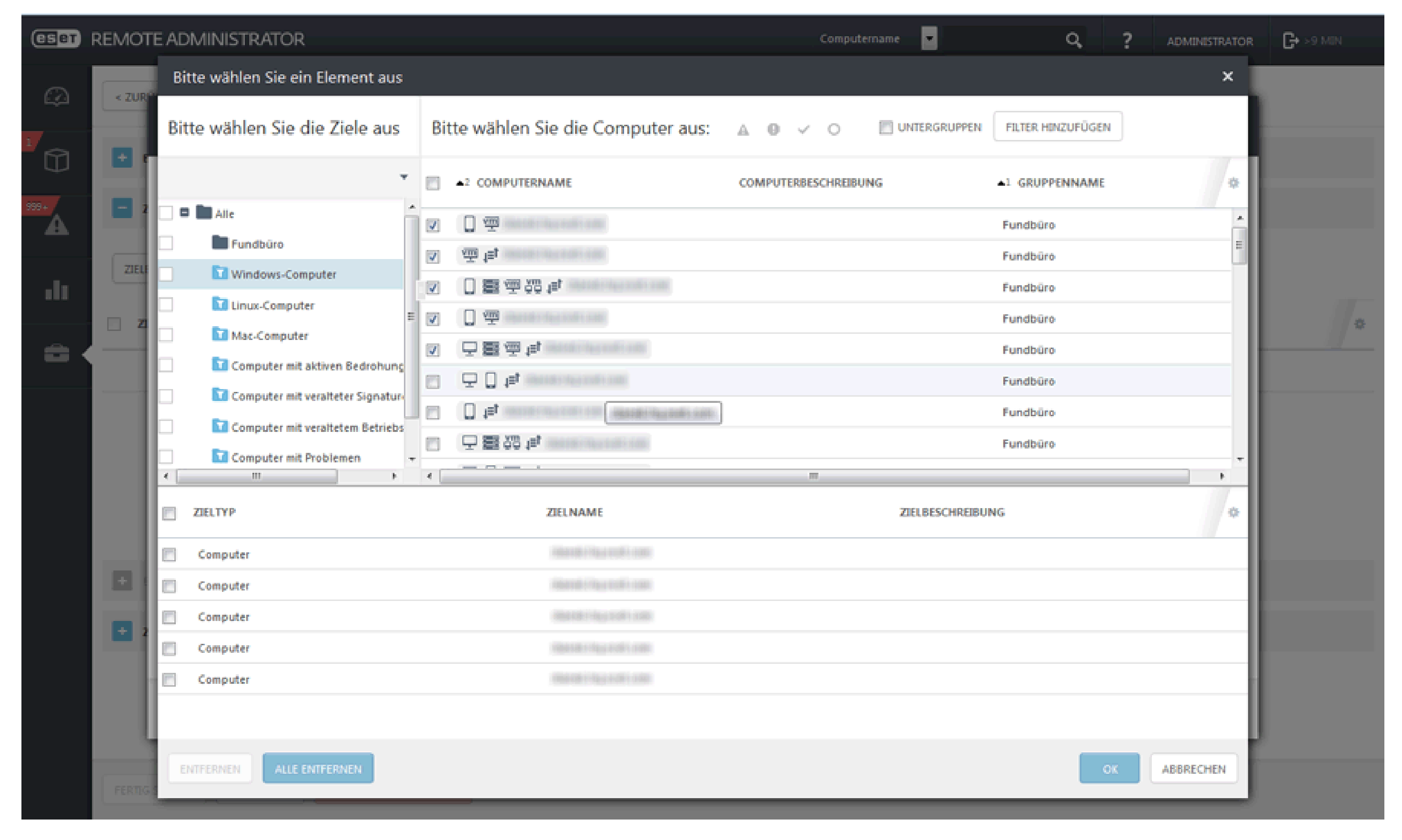
Manchmal kann ein Update der Signaturdatenbank Probleme verursachen oder Sie möchten ein Update aus bestimmten Gründen (zum Beispiel zum Testen oder Verwenden von Test-Updates) nicht auf allen Clients anwenden. In diesem Fall können Sie den Task **Rollback eines Updates der Signaturdatenbank** ausführen. Dieser Task setzt die Signaturdatenbank auf eine frühere Version zurück.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Hier können Sie die Einstellungen für den Rollback des Updates der Signaturdatenbank anpassen.

Aktion

- **Aktivierte Updates** – Updates sind aktiviert. Der Client empfängt das nächste Update der Signaturdatenbank.
- **Rollback ausführen und Aktualisierungen deaktivieren für** – Updates sind für den im Dropdown-Menü **Intervall deaktivieren** angegebenen Zeitraum deaktiviert (24, 36 oder 48 Stunden oder bis zur Aufhebung). Verwenden Sie die Option „Bis zur Aufhebung“ mit Vorsicht, da sie mit einem Sicherheitsrisiko verbunden ist.

Zusammenfassung

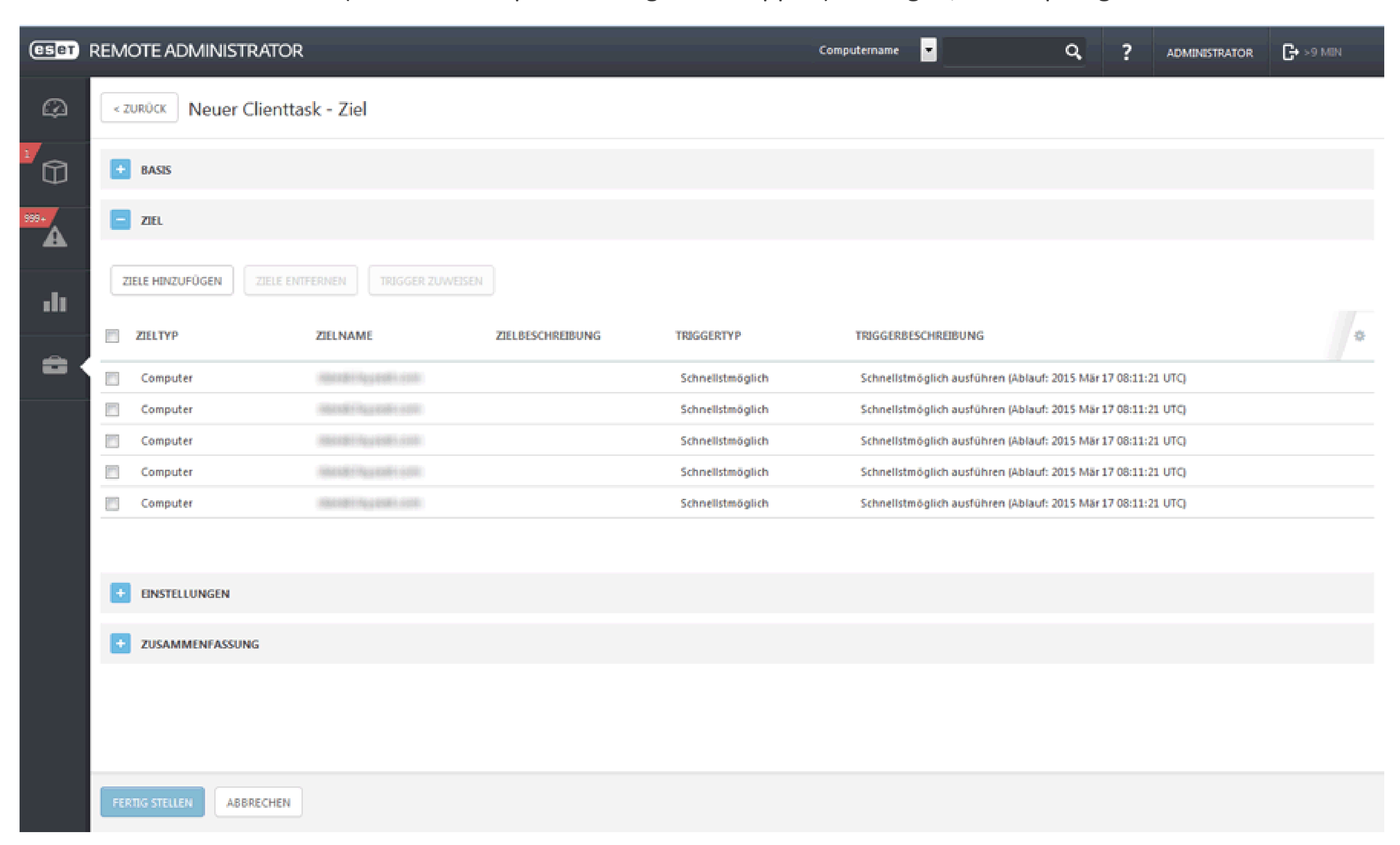
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.16 Anzeigen einer Meldung

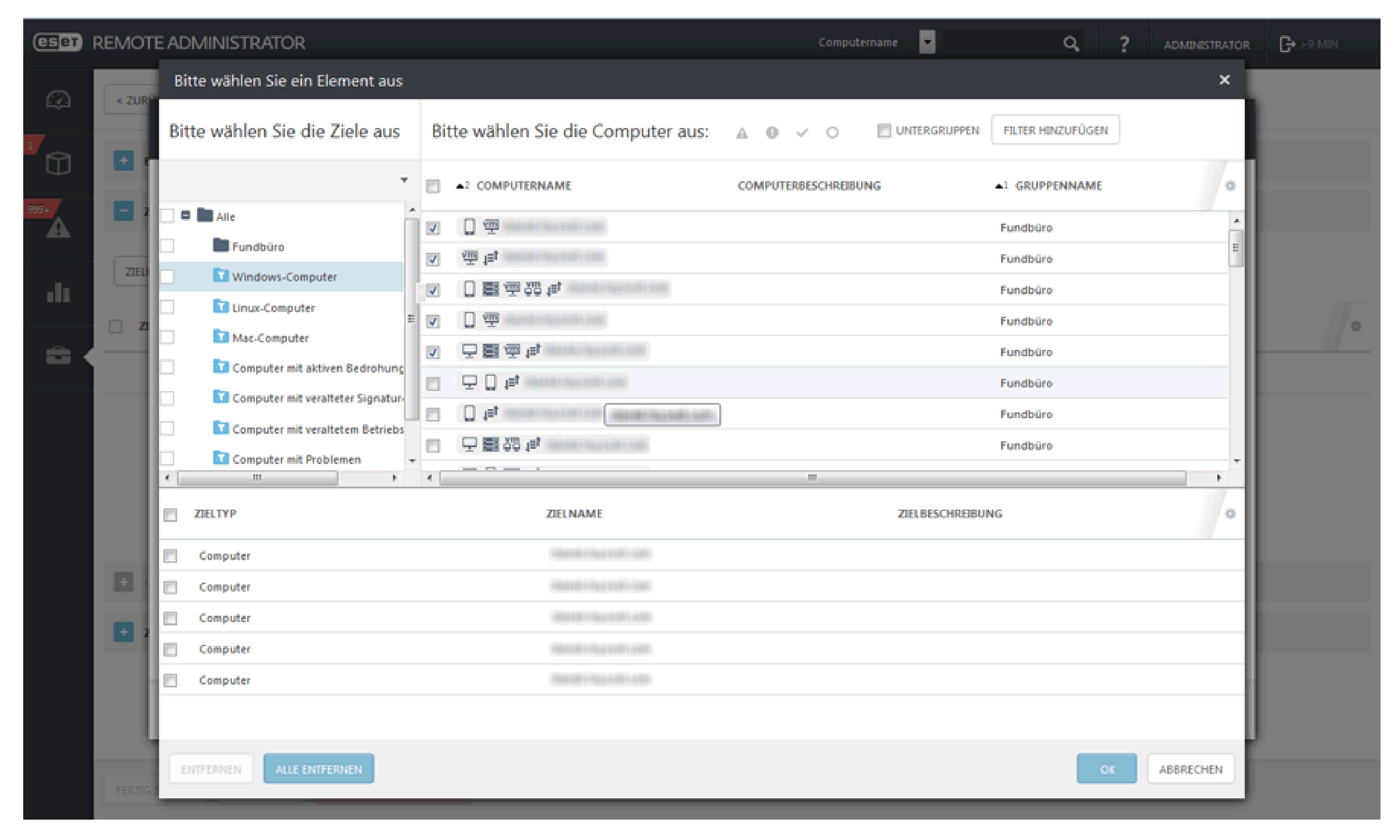
Mit dieser Funktion können Sie eine Nachricht an ein beliebiges Gerät (Clientcomputer, Tablet, Mobiltelefon usw.) senden. Die Nachricht wird auf dem Bildschirm des Geräts angezeigt, um dem Benutzer eine Information mitzuteilen.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Geben Sie einen **Titel** und die **Nachricht** ein.

Zusammenfassung

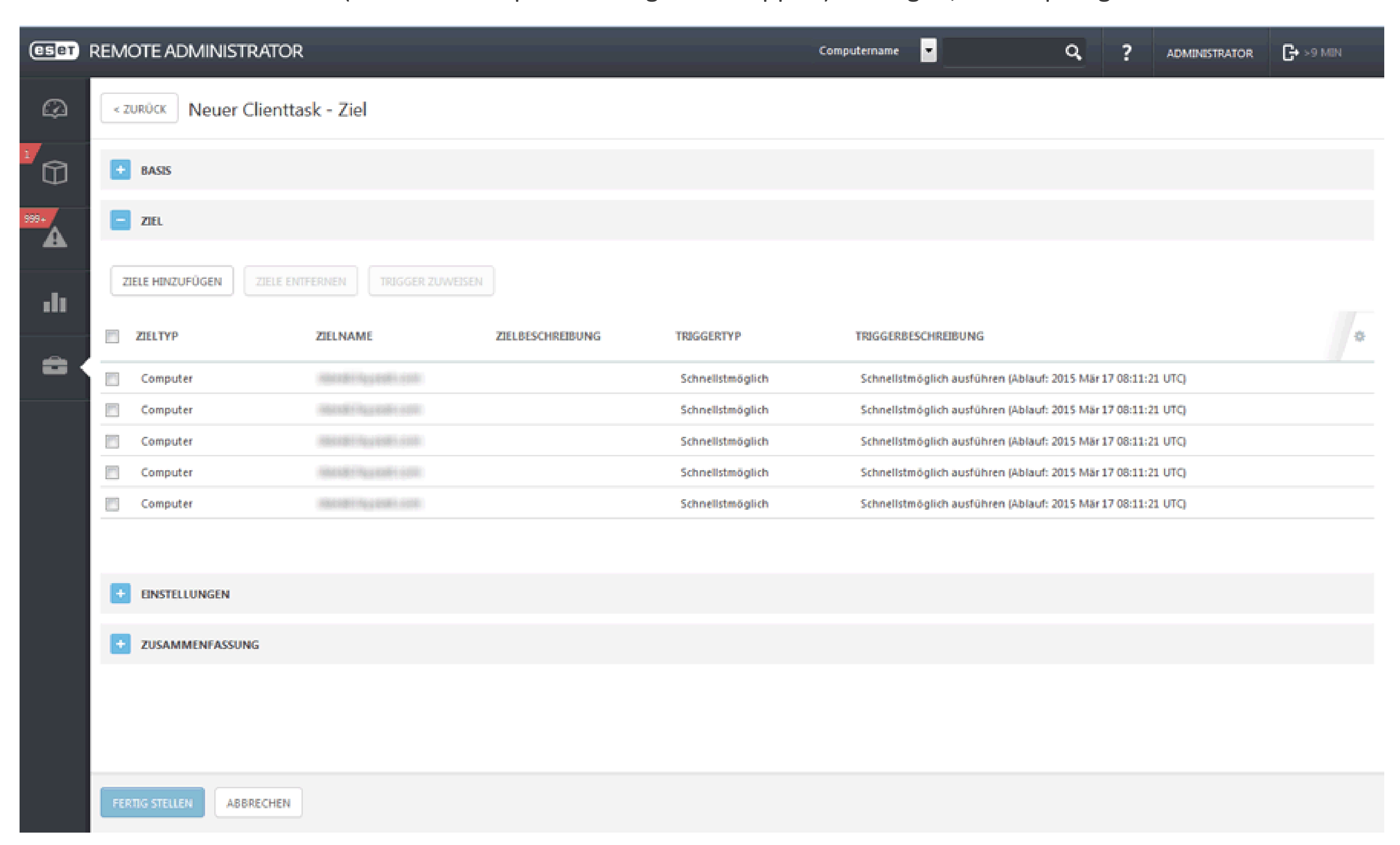
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.17 Anti-Theft-Aktion

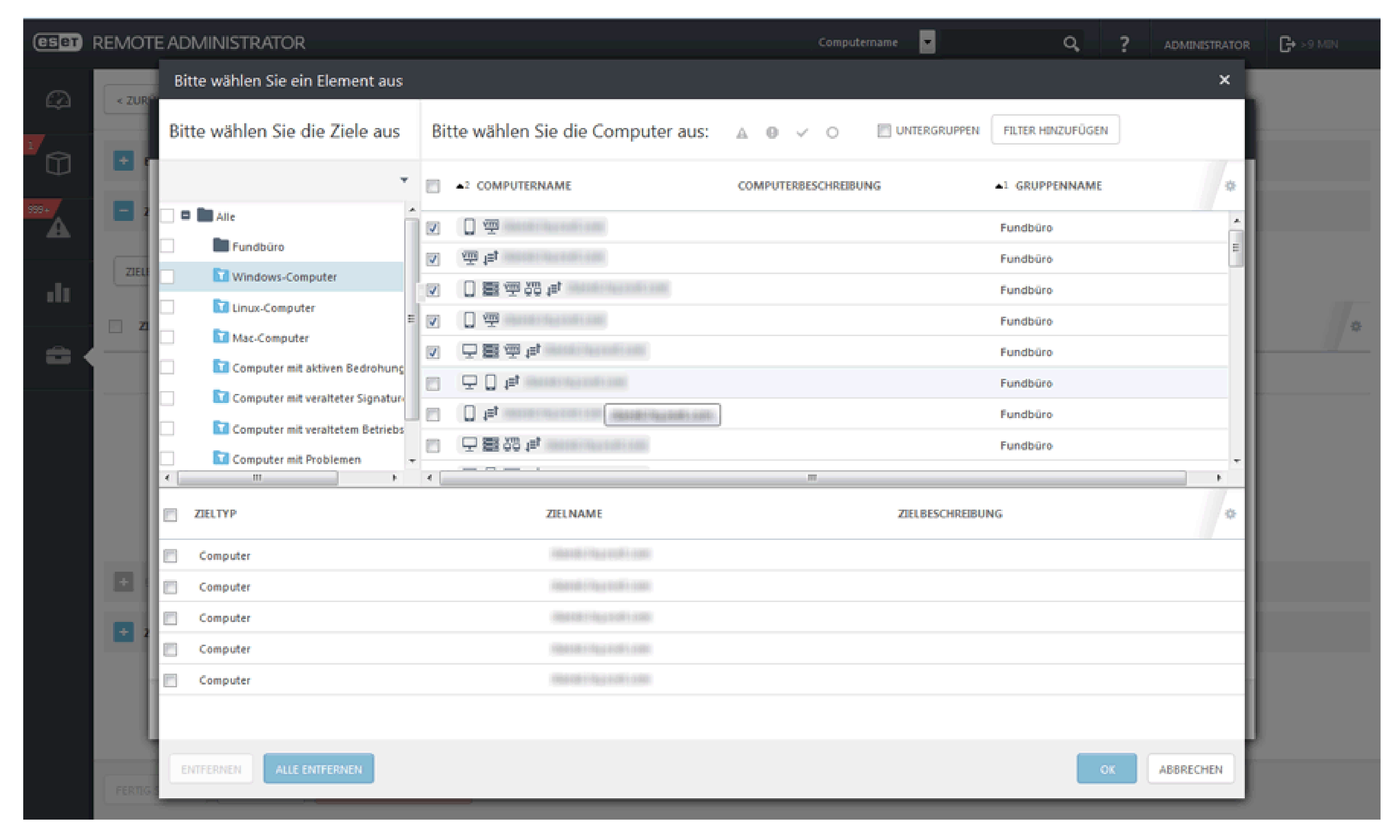
Die **Anti-Theft**-Funktion schützt Ihr Mobilgerät vor unbefugtem Zugriff. Wenn ein (registriertes und von ERA verwaltetes) Mobilgerät verloren oder gestohlen wird, werden bestimmte Aktionen automatisch ausgeführt. Weitere Aktionen können über Client-Tasks ausgeführt werden. Wenn eine nicht autorisierte Person eine vertrauenswürdige SIM-Karte durch eine nicht vertrauenswürdige SIM-Karte ersetzt, wird das Gerät von ESET Endpoint Security für Android **gesperrt** und eine SMS-Benachrichtigung wird an die vom Benutzer festgelegte(n) Telefonnummer(n) gesendet. Die Benachrichtigung enthält die Telefonnummer der aktuell verwendeten SIM-Karte, die **IMSI** (International Mobile Subscriber Identity) und die **IMEI** (International Mobile Equipment Identity) des Telefons. Der nicht autorisierte Benutzer weiß nicht, dass diese Meldung gesendet wurde, da sie automatisch aus den Nachrichtenlisten auf dem Gerät gelöscht wird. Sie können außerdem die **GPS**-Koordinaten des verlorenen Mobilgeräts anfordern oder mit einem Clienttask remote alle auf dem Gerät gespeicherten Daten löschen.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

- **Suchen** - Das Gerät antwortet mit einer Textnachricht, die die GPS-Koordinaten des Geräts enthält. Wenn nach 10 Minuten eine genauere Standortangabe verfügbar ist, sendet das Gerät die Nachricht erneut.
- **Sperren** - Das Gerät wird gesperrt. Das Gerät kann mit dem Administratorpasswort oder dem Entsperrbefehl entsperrt werden.
- **Entsperren -** Das Gerät wird entsperrt, sodass es wieder verwendet werden kann. Die aktuell im Gerät eingelegte SIM-Karte wird als vertrauenswürdige SIM-Karte gespeichert.
- **Alarm -** Das Gerät wird gesperrt und gibt 5 Minuten lang (oder bis zur Entsperrung) einen sehr lauten Ton aus.
- **Daten löschen -** Alle zugreifbaren Daten auf dem Gerät werden gelöscht (Datei wird überschrieben). ESET Endpoint Security bleibt auf dem Gerät erhalten. Dies kann mehrere Stunden in Anspruch nehmen.
- **Erweiteres Zurücksetzen auf Werkseinstellungen** - Alle zugreifbaren Daten auf dem Gerät werden gelöscht (Dateikopfdaten werden zerstört) und das Gerät wird auf die standardmäßigen Werkseinstellungen zurückgesetzt. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen", wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.2.18 Geräteregistrierung

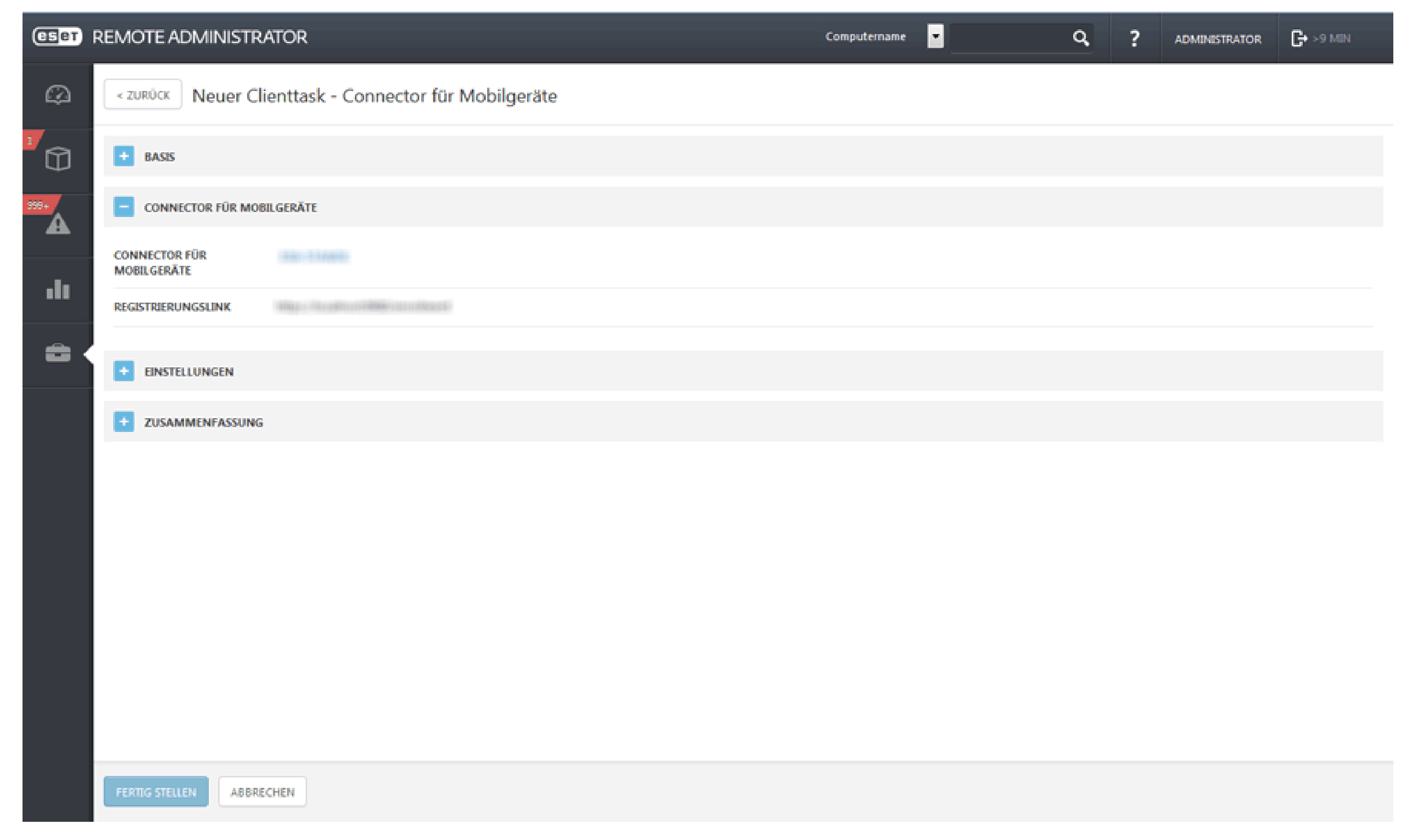
Mobiltelefone können vom ERA-Server mithilfe der Mobil-App ESET Endpoint Security für Android Version 2 verwaltet werden. Um mobile Geräte zu verwalten, müssen Sie sie zuerst bei ERA registrieren. Die Geräteregistrierung wird mithilfe eines Client-Tasks ausgeführt.

Basis

Geben Sie einen **Namen** und (optional) eine **Beschreibung** für den Task ein.

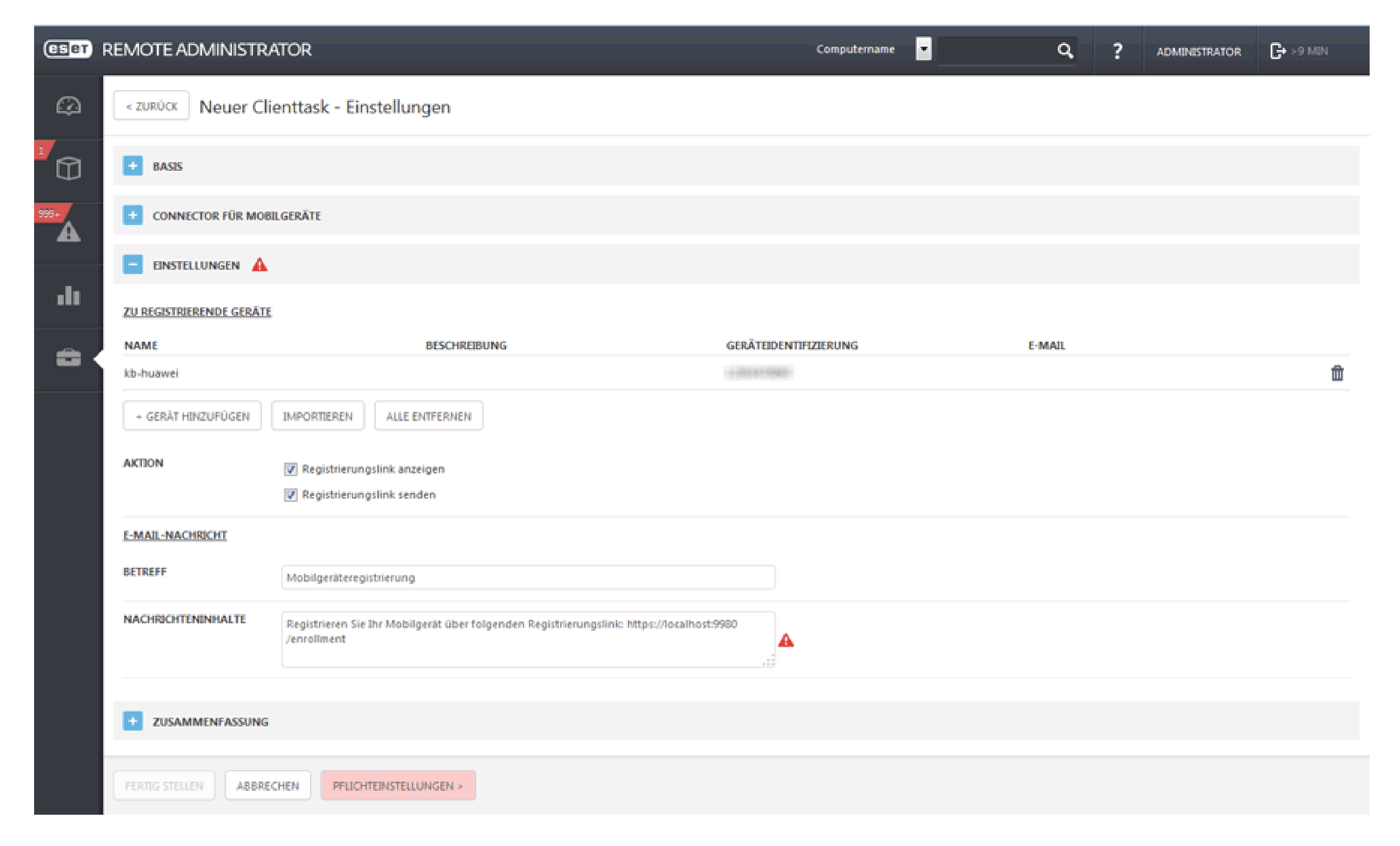
Connector für Mobilgeräte

Klicken Sie auf **Auswählen** und wählen Sie den Computer aus, auf dem der Connector für Mobilgeräte installiert ist. Es wird automatisch ein Registrierungslink (URL) angezeigt. Wenn nach dem Klicken auf „Auswählen" keine Links angezeigt werden, überprüfen Sie, ob der Server des Connectors für Mobilgeräte erreichbar ist. Wenn der Connector für Mobilgeräte noch nicht installiert ist, beachten Sie die Installationshinweise in den Kapiteln Installation des Connectors für Mobilgeräte - Windows und Installation des Connectors für Mobilgeräte - Linux in diesem Handbuch.



Einstellungen

Geben Sie den **Namen** des Mobilgeräts (dieser Name wird in der Liste der Computer angezeigt) und optional eine **Beschreibung** ein. Geben Sie die IMEI-Nummer des Mobilgeräts ein, das Sie hinzufügen möchten. Es empfiehlt sich, auch eine **E-Mail-Adresse** einzugeben, die mit dem Konto verknüpft wird (der Registrierungslink wird an diese E-Mail-Adresse gesendet). Klicken Sie auf **+ Gerät hinzufügen**, wenn Sie ein weiteres Mobilgerät hinzufügen möchten. Sie können mehrere Geräte gleichzeitig hinzufügen. Legen Sie eine **Aktion** fest, indem Sie das Kontrollkästchen neben **Registrierungslink anzeigen** und/oder **Registrierungslink senden** (die URL wird an die mit dem Gerät verknüpfte(n) E-Mail-Adresse(n) gesendet) auswählen. Wenn Sie einen Registrierungslink an das Mobilgerät senden möchten (empfohlen), können Sie den **Betreff** und den **Nachrichteninhalt** bearbeiten. Achten Sie jedoch darauf, die Registrierungs-URL nicht zu ändern.



Zusammenfassung

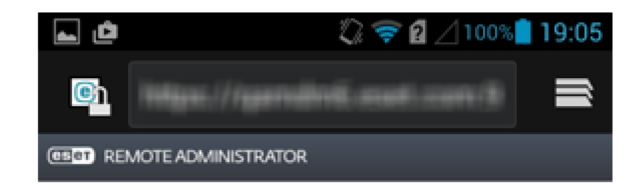
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

Klicken Sie auf **Fertig stellen**. Der Registrierungslink (URL) wird angezeigt. Wenn Sie keine E-Mail-Adresse festlegen und nicht **Registrierungslink senden** ausgewählt haben, müssen Sie die URL entweder manuell im Webbrowser auf dem Mobilgerät eingeben oder die URL auf eine andere Weise an das Mobilgerät senden.

Bei der Aktivierung von ESET Endpoint Security für Android (EESA) auf dem Mobilgerät stehen zwei Verfahren zur Registrierung zur Verfügung. Sie können EESA auf dem Mobilgerät mit dem ERA-Clienttask für die Produktaktivierung aktivieren (empfohlen). Das zweite Verfahren ist für Mobilgeräte anwendbar, auf der die EESA-App bereits aktiviert ist.

EESA noch nicht aktiviert - Befolgen Sie die nachfolgenden Schritte, um das Produkt zu aktivieren und Ihr Gerät zu registrieren:

1. Tippen Sie auf die URL des Registrierungslinks, den Sie per E-Mail erhalten haben, oder geben Sie die URL manuell in den Browser ein. Fügen Sie auch die Portnummer hinzu (zum Beispiel https://eramdm:9980). Möglicherweise werden Sie aufgefordert, ein SSL-Zertifikat zu akzeptieren. Klicken Sie auf „Akzeptieren“, wenn Sie zustimmen, und dann auf **Verbinden**.



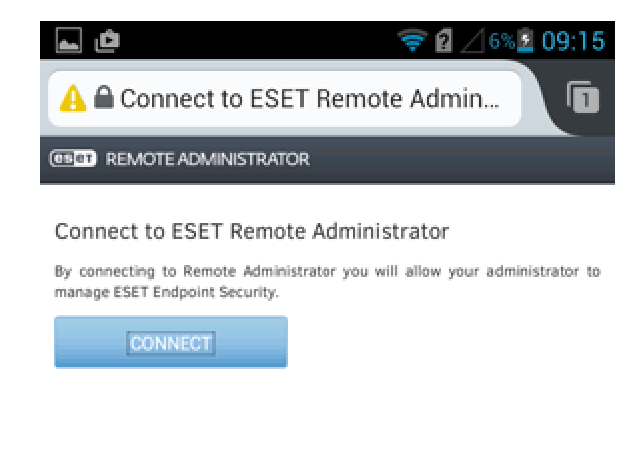
Connect to ESET Remote Administrator

By connecting to Remote Administrator you will allow your administrator to manage ESET Endpoint Security.

CONNECT

2. Wenn ESET Endpoint Security nicht auf dem Mobilgerät installiert ist, werden Sie automatisch zu Google Play Store weitergeleitet, wo Sie die App herunterladen können.

HINWEIS: Wenn Sie die Benachrichtigung **Keine App zum Öffnen der URL gefunden** erhalten, versuchen Sie, den Registrierungslink im standardmäßigen Android-Webbrowser zu öffnen.



3. Geben Sie den Namen des Mobilgerätebenutzers ein.





4. Tippen Sie auf **Aktivieren**, um den Deinstallationsschutz zu aktivieren.



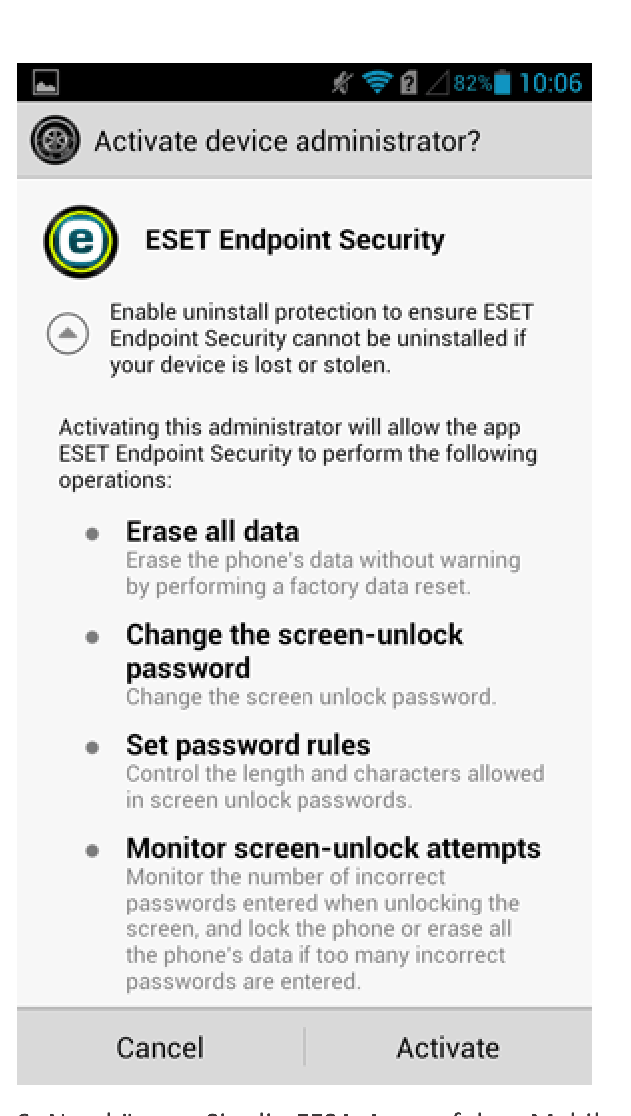
Enable uninstall protection

Enable uninstall protection to ensure ESET Endpoint Security cannot be uninstalled if your device is lost or stolen.

You will be required to set ESET Endpoint Security as device administrator.

Enable

5. Tippen Sie auf **Aktivieren**, um dem Geräteadministrator zu aktivieren.



6. Nun können Sie die EESA-App auf dem Mobilgerät beenden und die ERA-Webkonsole öffnen.



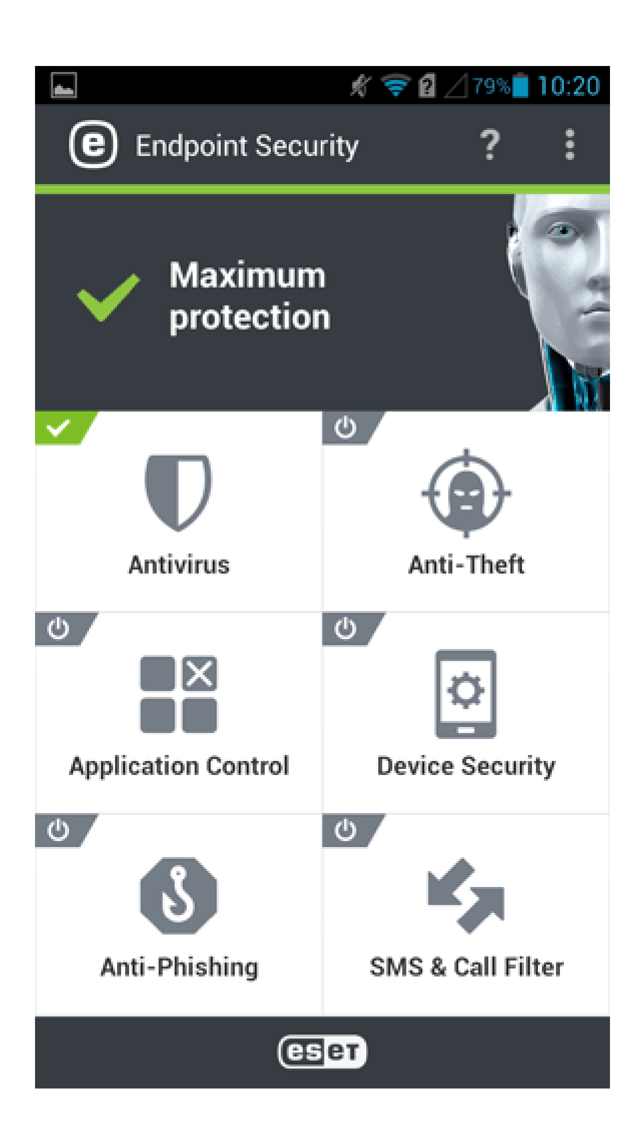


7. Wechseln Sie in der ERA-Webkonsole zu **Admin** > **Client-Tasks** > **Mobilgerät** > Produktaktivierung und klicken Sie auf **Neu**.

8. Wählen Sie das Mobilgerät aus, indem Sie auf **Ziele hinzufügen** klicken.

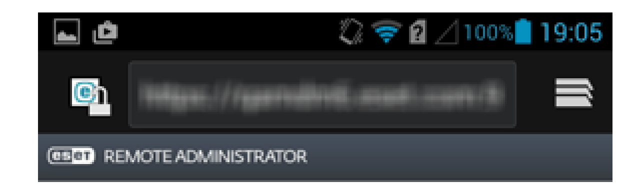
9. Klicken Sie unter „Einstellungen“ auf <ESET-Lizenz auswählen> und wählen Sie die geeignete Lizenz aus. Klicken Sie auf **Fertig stellen**.

Das Ausführen des Client-Tasks zur Produktaktivierung auf dem Mobilgerät kann einige Zeit in Anspruch nehmen. Nachdem der Task erfolgreich ausgeführt wurde, ist die EESA-App aktiviert und das Mobilgerät wird von ERA verwaltet. Der Benutzer kann nun die EESA-App verwenden. Nach dem Öffnen der EESA-App wird das Hauptmenü angezeigt:



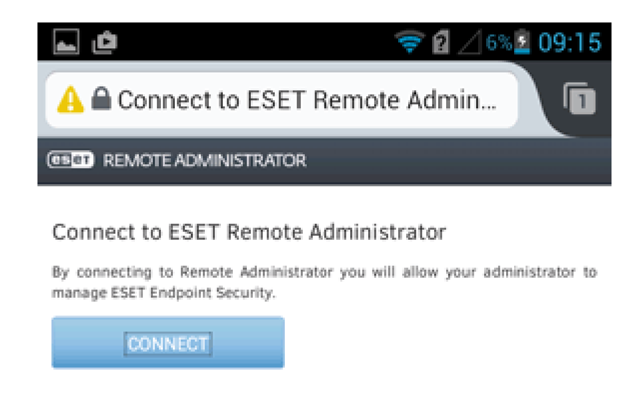
EESA bereits aktiviert - Befolgen Sie diese Schritte, um das Gerät zu registrieren:

1. Tippen Sie auf die URL des Registrierungslinks, den Sie per E-Mail erhalten haben, oder geben Sie die URL manuell in den Browser ein. Fügen Sie auch die Portnummer hinzu (zum Beispiel *https://eramdm:9980*). Möglicherweise werden Sie aufgefordert, ein SSL-Zertifikat zu akzeptieren. Klicken Sie auf „Akzeptieren“, wenn Sie zustimmen, und dann auf **Verbinden**.



HINWEIS: Wenn ESET Endpoint Security nicht auf dem Mobilgerät installiert ist, werden Sie automatisch zu Google Play Store weitergeleitet, wo Sie die App herunterladen können.

HINWEIS: Wenn Sie die Benachrichtigung **Keine App zum Öffnen der URL gefunden** erhalten, versuchen Sie, den Registrierungslink im standardmäßigen Android-Webbrowser zu öffnen.



2. Überprüfen Sie die Verbindungsdetails (Serveradresse und Port des Connectors für Mobilgeräte) und klicken Sie auf **Verbinden**.



Connect to Remote Administrator server

Specify the server connection info that you received from your admin.

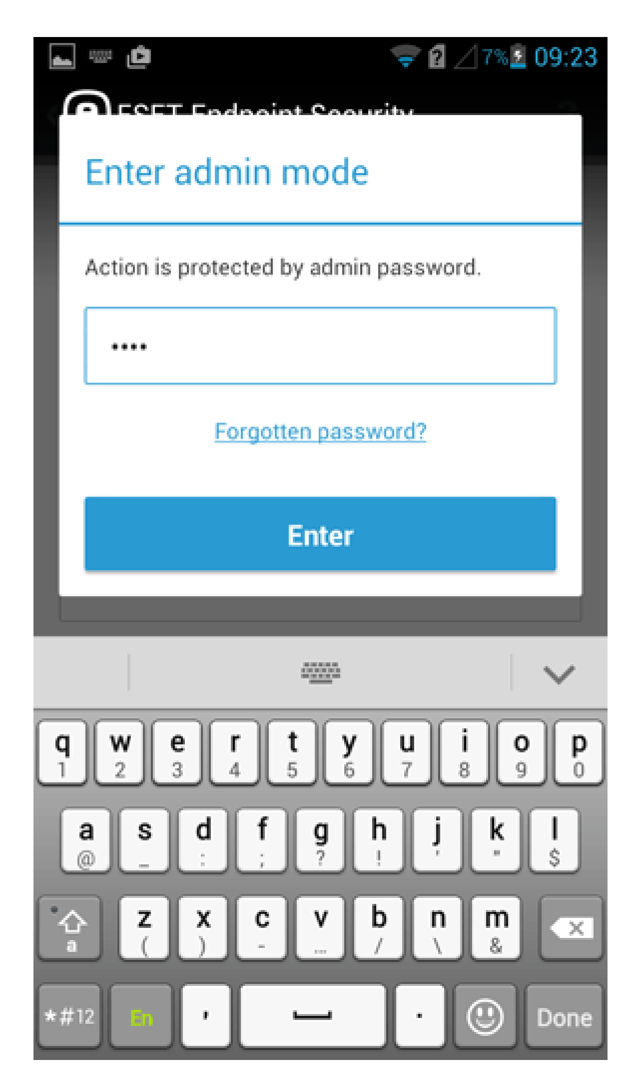
SERVER ADDRESS



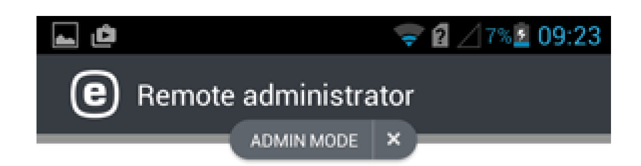
9980

Connect

3. Geben Sie das Passwort für den Administratormodus von ESET Endpoint Security in das leere Feld ein und tippen Sie auf die Eingabeschaltfläche.



4. Das Mobilgerät wird nun von ERA verwaltet. Tippen Sie auf „Fertig stellen“.





6.1.3.2.19 Verwaltung beenden (ERA-Agent deinstallieren)

- **Desktop** - Mit diesem Task wird der Agent, der auf dem Computer mit MDM installiert ist, entfernt.
- **Mobilgerät** - Dieser Task hebt die MDM-Registrierung des Mobilgeräts auf.

Nachdem das Gerät nicht mehr verwaltet wird (Agent wurde entfernt), können in den verwalteten Produkten einige Einstellungen verbleiben.
Es empfiehlt sich, bestimmte Einstellungen (z. B. für den Passwortschutz) mithilfe einer Policy auf den Standardwert zurückzusetzen, bevor das Gerät von der Verwaltung ausgeschlossen wird. Außerdem werden alle auf dem Agenten ausgeführten Tasks abgebrochen. Der Ausführungsstatus **Wird ausgeführt**, **Fertig** oder **Fehler des Tasks** wird je nach Replikation möglicherweise nicht richtig in der ERA Web-Konsole angezeigt.

1. Wenn einige besondere Einstellungen auf dem Gerät nicht beibehalten werden sollen, legen Sie eine Geräte-Policy so fest, dass die unerwünschten Einstellungen auf Standardwerte (bzw. auf die gewünschten Werte) gesetzt werden.
2. Bevor Sie diesen Schritt ausführen, warten Sie lange genug, um sicher zu sein, dass die Policies aus Punkt 1 die Replikation auf dem Zielcomputer abgeschlossen haben, bevor Sie den Computer in ERA aus der Liste löschen.
3. Vor dem Ausführen dieses Schritts sollten Sie lang genug warten, um sicher zu sein, dass die Policies aus Punkt 2 die Replikation auf dem Zielcomputer abgeschlossen haben.

HINWEIS: Für diesen Task sind keine Einstellungen verfügbar.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.

Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.

Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Zusammenfassung

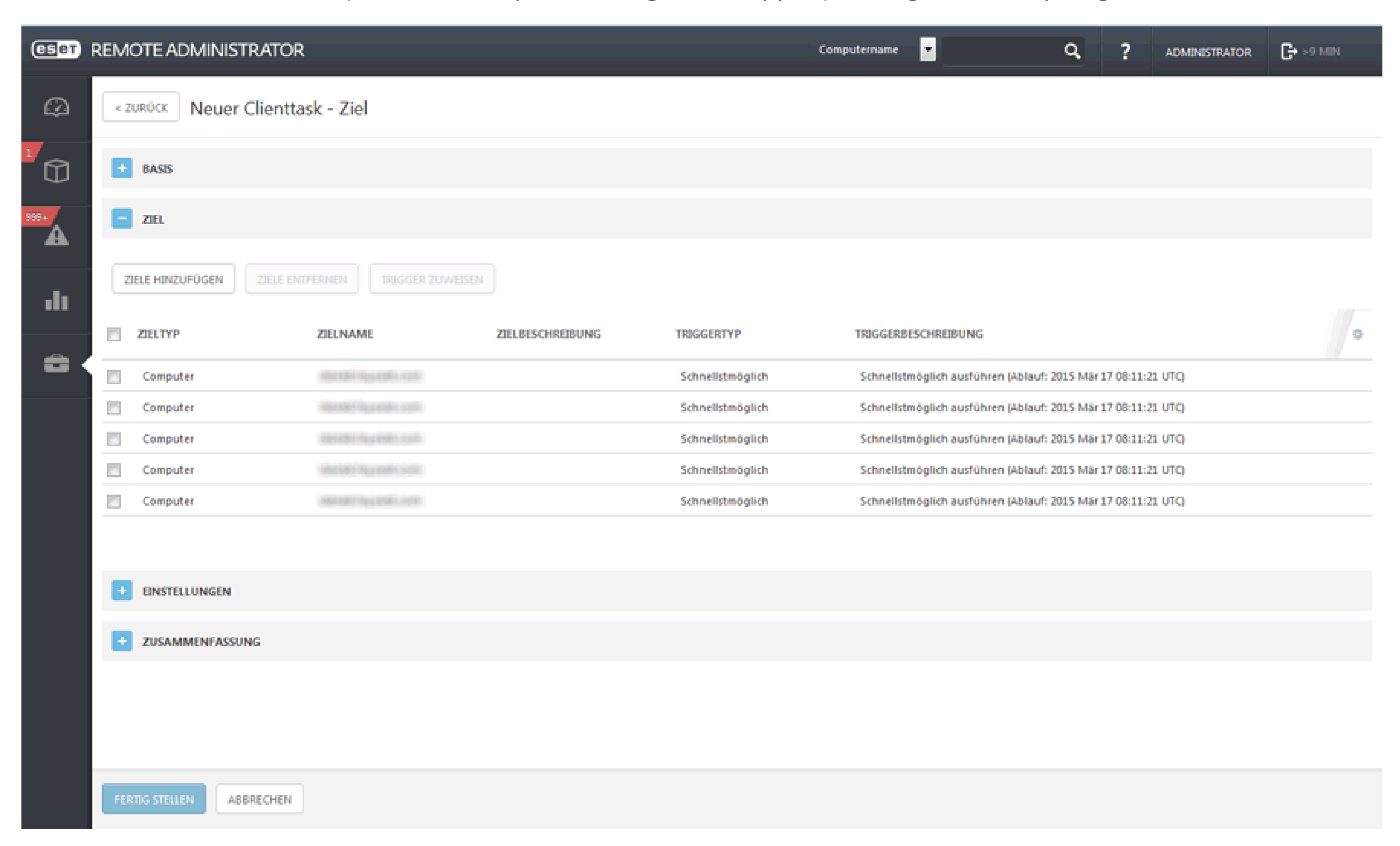
Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.3 Konfiguration verwalteter Produkte exportieren

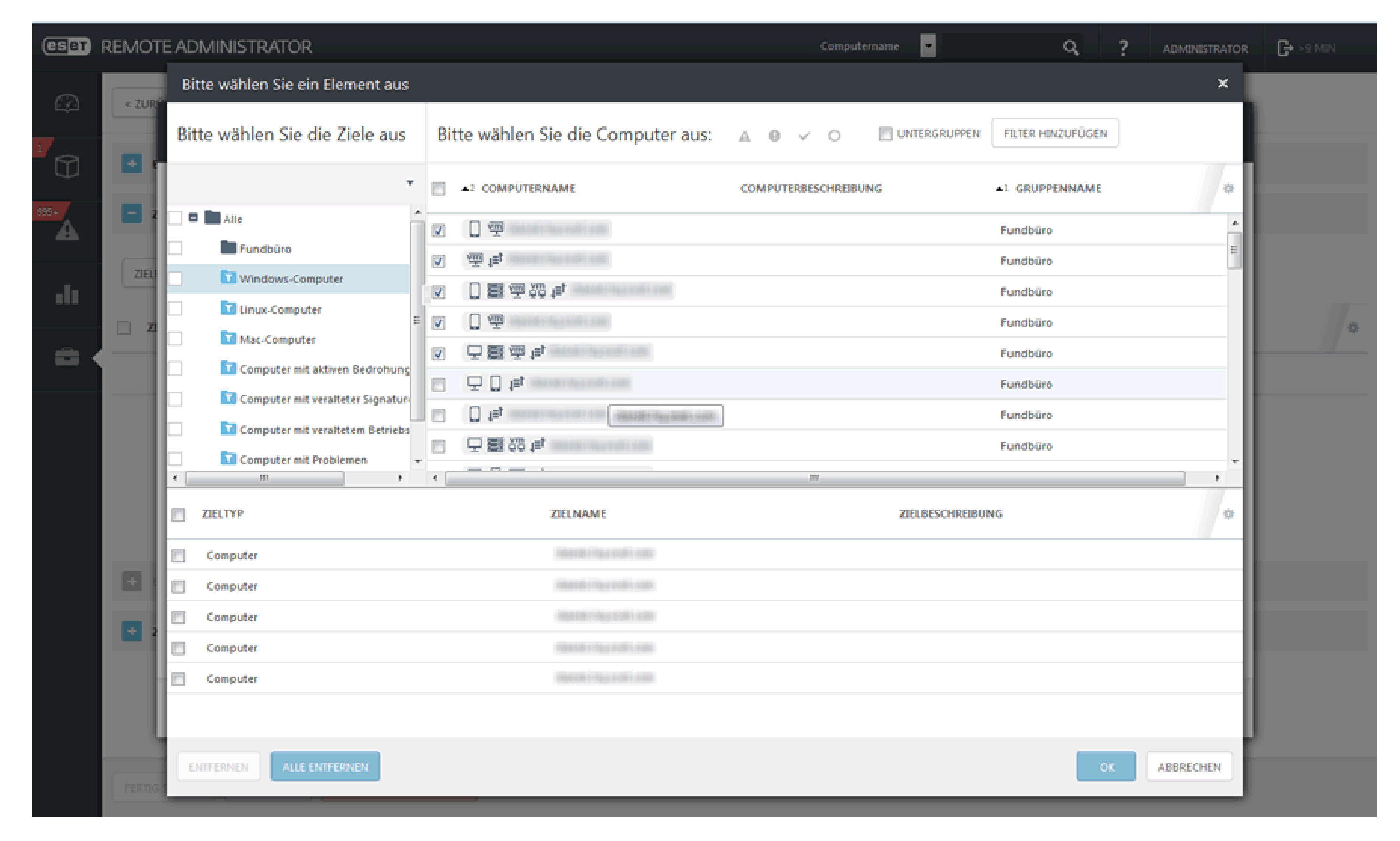
Mit dem Task **Konfiguration verwalteter Produkte exportieren** können Sie die Einstellungen einzelner ERA-Komponenten oder auf den Clients installierter ESET-Sicherheitsprodukte exportieren.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel“ ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Einstellungen

Konfigurationseinstellungen für verwaltete Produkte exportieren

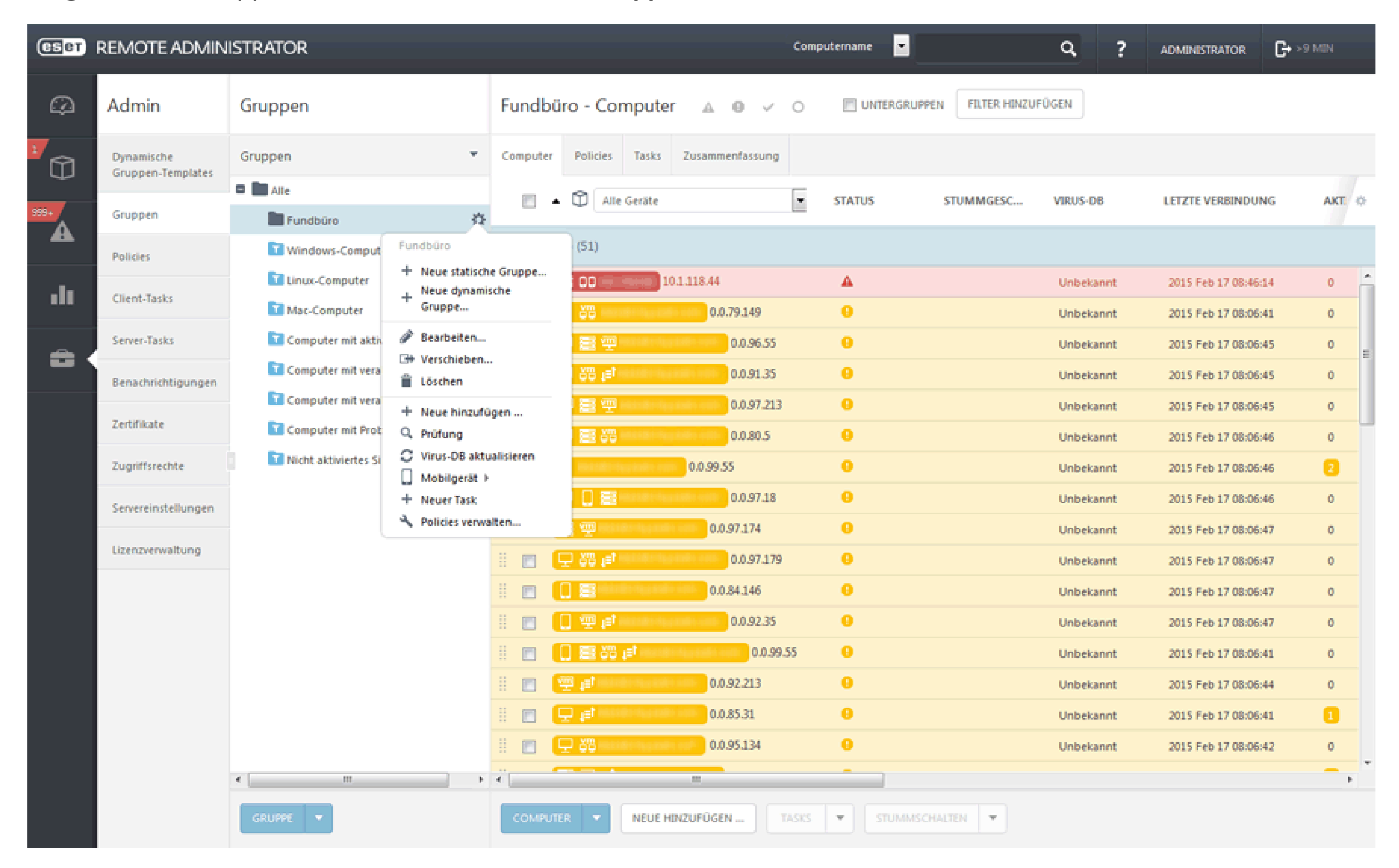
- **Produkt** – Wählen Sie eine ERA-Komponente oder ein Sicherheitsprodukt auf einem Client aus, für die/das die Konfiguration exportiert werden soll.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

6.1.3.4 Zuweisen eines Task zu einer Gruppe

Klicken Sie auf **Admin** > **Gruppen**, wählen Sie eine **Statische** oder **Dynamische** Gruppe aus ⚙ neben der ausgewählten Gruppe. Klicken Sie alternativ auf **Gruppe** > + **Neuer Task**



Sie können auch unter **Computer** eine **Statische** oder **Dynamische** Gruppe auswählen und auf ⚙ > + **Neuer Task** klicken.

Der Assistent für neue Client-Tasks wird geöffnet.

6.1.3.5 Zuweisen eines Tasks zu Computern

Tasks können auf drei verschiedene Weisen einem oder mehreren Computern zugewiesen werden.

1. **Dashboard** > **Computer mit Problemen**> + **Neuer Task ...**

2. **Computer** > Computer über die Kontrollkästchen auswählen > + auswählen **Neuer Task ...**

3. **Admin**> **Gruppen** > Computer auswählen > Schaltfläche **Tasks**, Aktion auswählen und auf **+** klicken **Neuer Task ...**

Ein Fenster mit dem Assistenten für neuen Clienttask wird geöffnet.

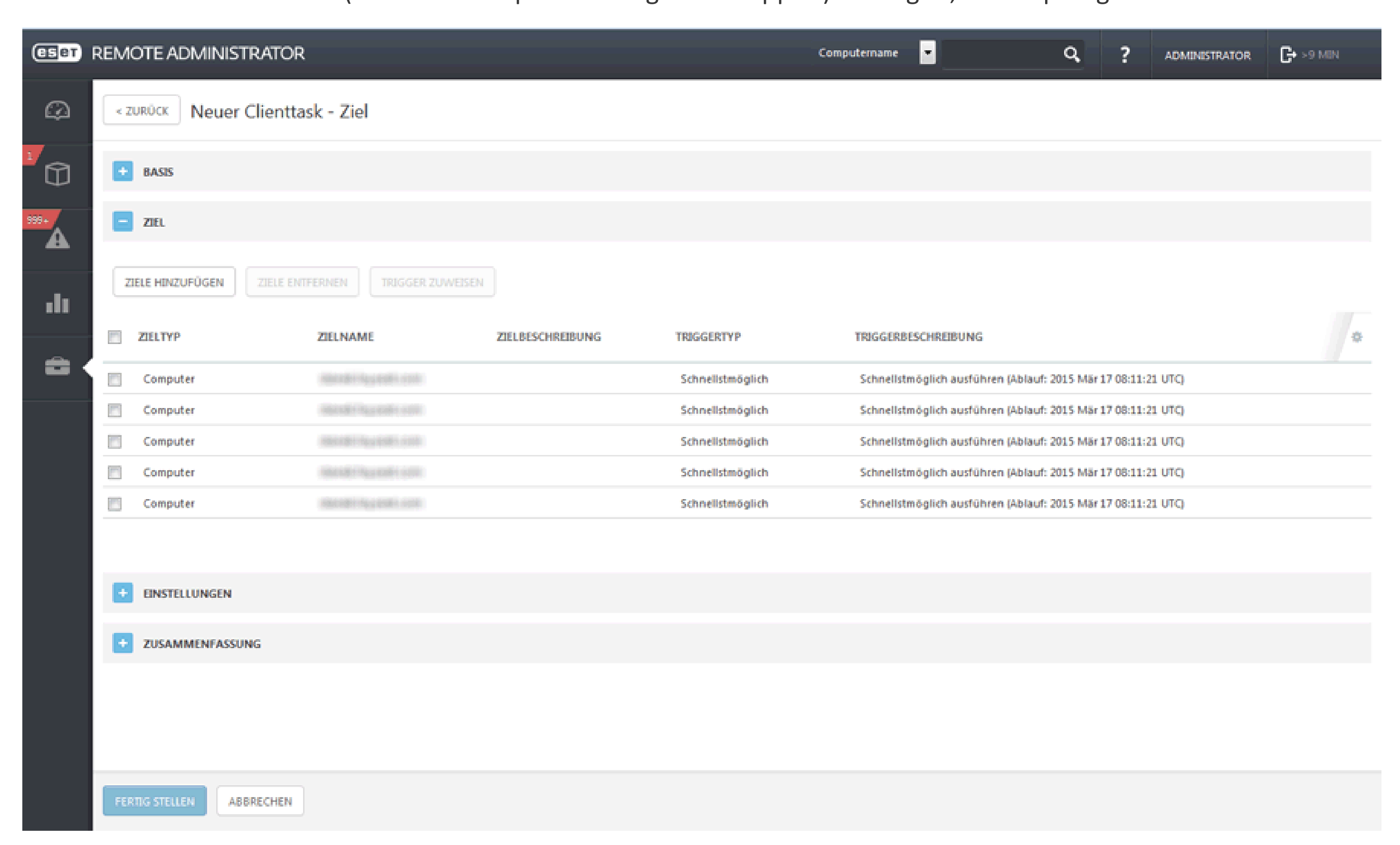
6.1.3.6 Planen eines Task

So erstellen Sie einen geplanten Task:

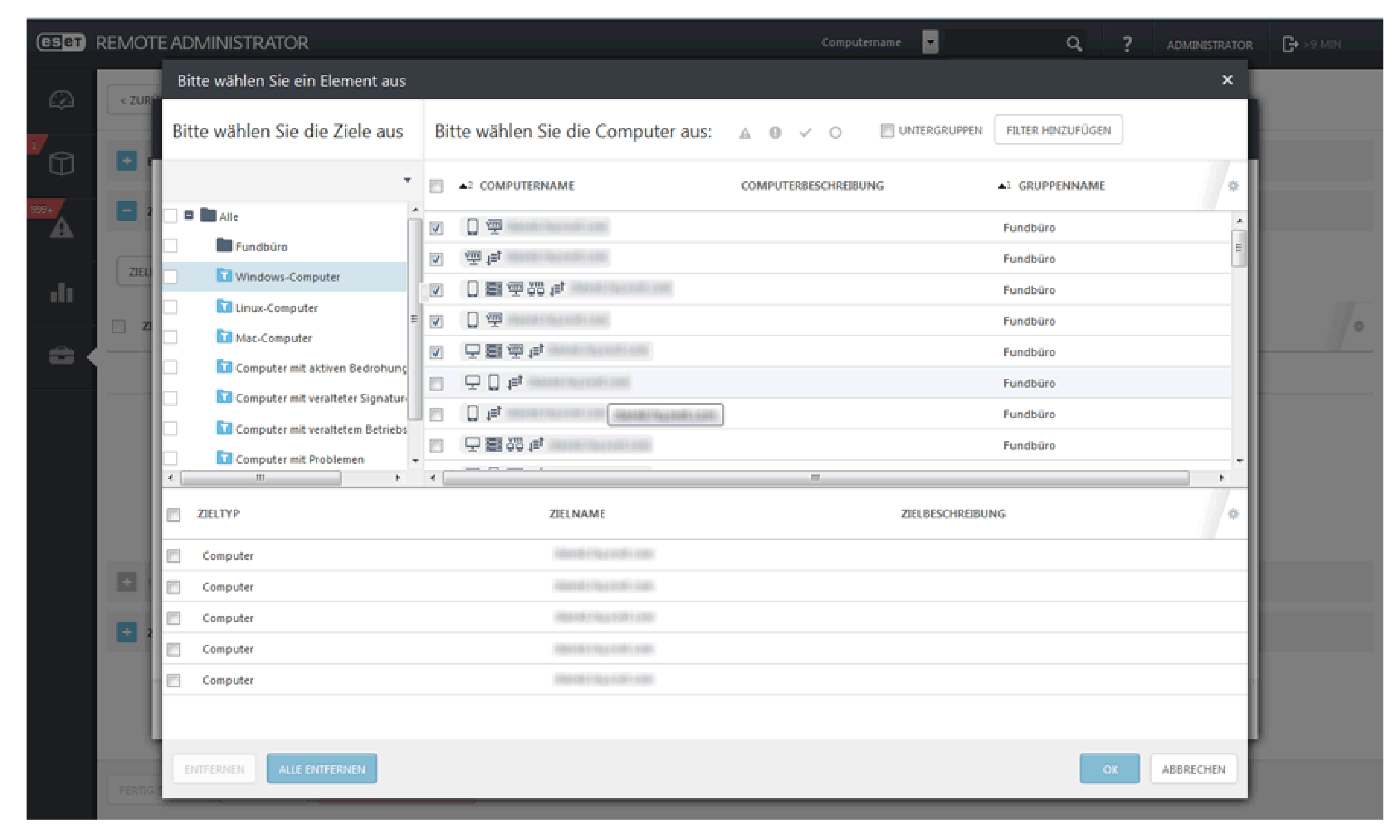
Navigieren Sie zu **Admin** > **Clienttasks**, wählen Sie **Task** aus und klicken Sie auf **Bearbeiten ...** Navigieren Sie zu **Ziel**.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.



Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.



Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger" fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

6.1.3.7 Trigger

Trigger können sowohl auf dem ERA-Server als auch auf den Agenten (Clients) verwendet werden.

6.1.4 Server-Tasks

Servertasks können zur Automatisierung von Routineaufgaben eingesetzt werden. Für Server-Tasks können Trigger konfiguriert werden, sodass der Task ausgeführt wird, sobald eine bestimmte Ereigniskombination auf dem ERA-Server auftritt.

Auf dem ERA-Server können folgende Arten von Tasks geplant werden:

- Synchronisierung statischer Gruppen aktualisiert die Clientinformationen in Gruppen, damit Sie mit aktuellen Daten arbeiten.
- Agenten-Bereitstellung verteilt den Agenten an die Clientcomputer.
- Bericht erstellen ermöglicht das sofortige Generieren von Berichten.

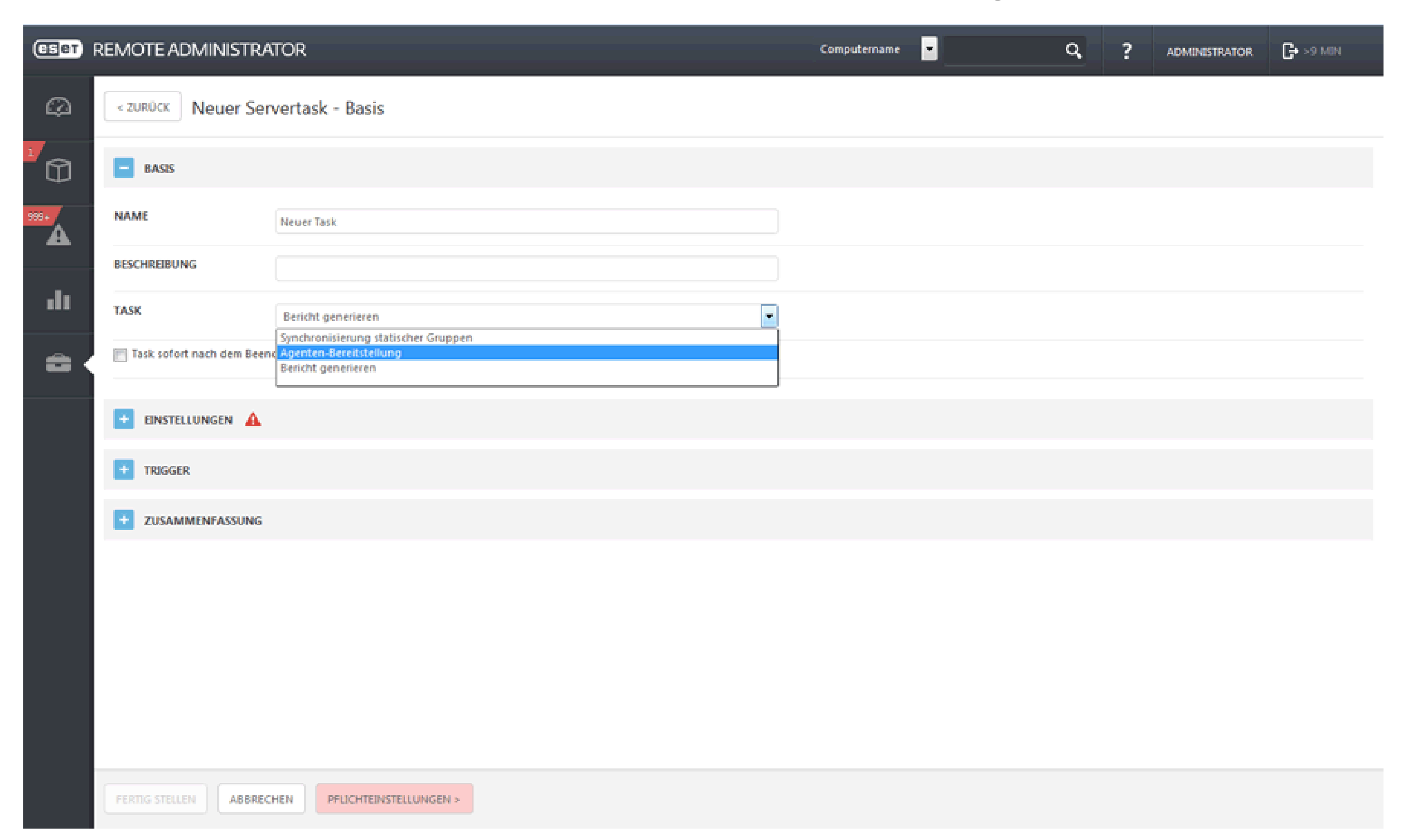
HINWEIS: Servertasks können nicht einem bestimmten Client oder einer bestimmten Clientgruppe zugewiesen werden.

6.1.4.1 Assistent für Server-Tasks

Um mit dem Erstellen eines neuen Tasks zu beginnen, klicken Sie auf **Admin** > **Server-Tasks** > **Neu**.

Basis

Geben Sie grundlegende Informationen zum Task ein, wie **Name**, **Beschreibung** (optional) und **Tasktyp**. Der **Tasktyp** legt die Einstellungen und das Verhalten des Tasks fest. Markieren Sie das Kontrollkästchen neben "Task sofort nach dem Beenden ausführen", um den Task sofort auszuführen, nachdem Sie auf "Fertig stellen" klicken.



6.1.4.2 Verwalten von Server-Tasks

Die folgenden vordefinierten Server-Tasks sind verfügbar:

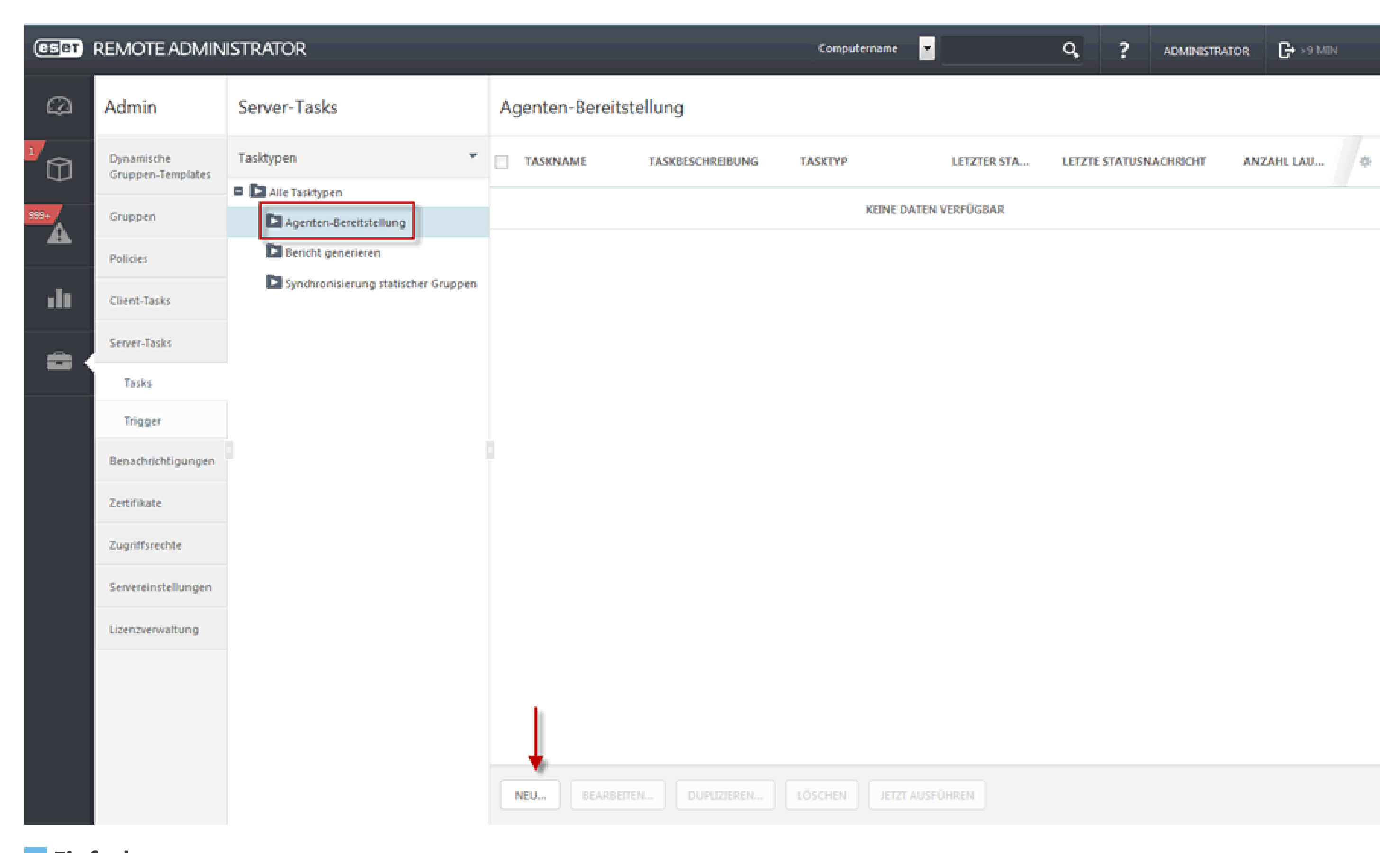
- Synchronisierung statischer Gruppen: aktualisiert die Gruppeninformationen, damit aktuelle Daten angezeigt werden.
- Agenten-Bereitstellung verteilt den Agenten an die Clientcomputer.
- Bericht erstellen ermöglicht das Generieren von Berichten nach Bedarf.

6.1.4.2.1 Agenten-Bereitstellung

Die Remote-Bereitstellung des ERA-Agenten wird im Bereich **Admin** ausgeführt. Führen Sie die folgenden Anweisungen aus oder sehen Sie sich das Anleitungsvideo in der Knowledgebase an.

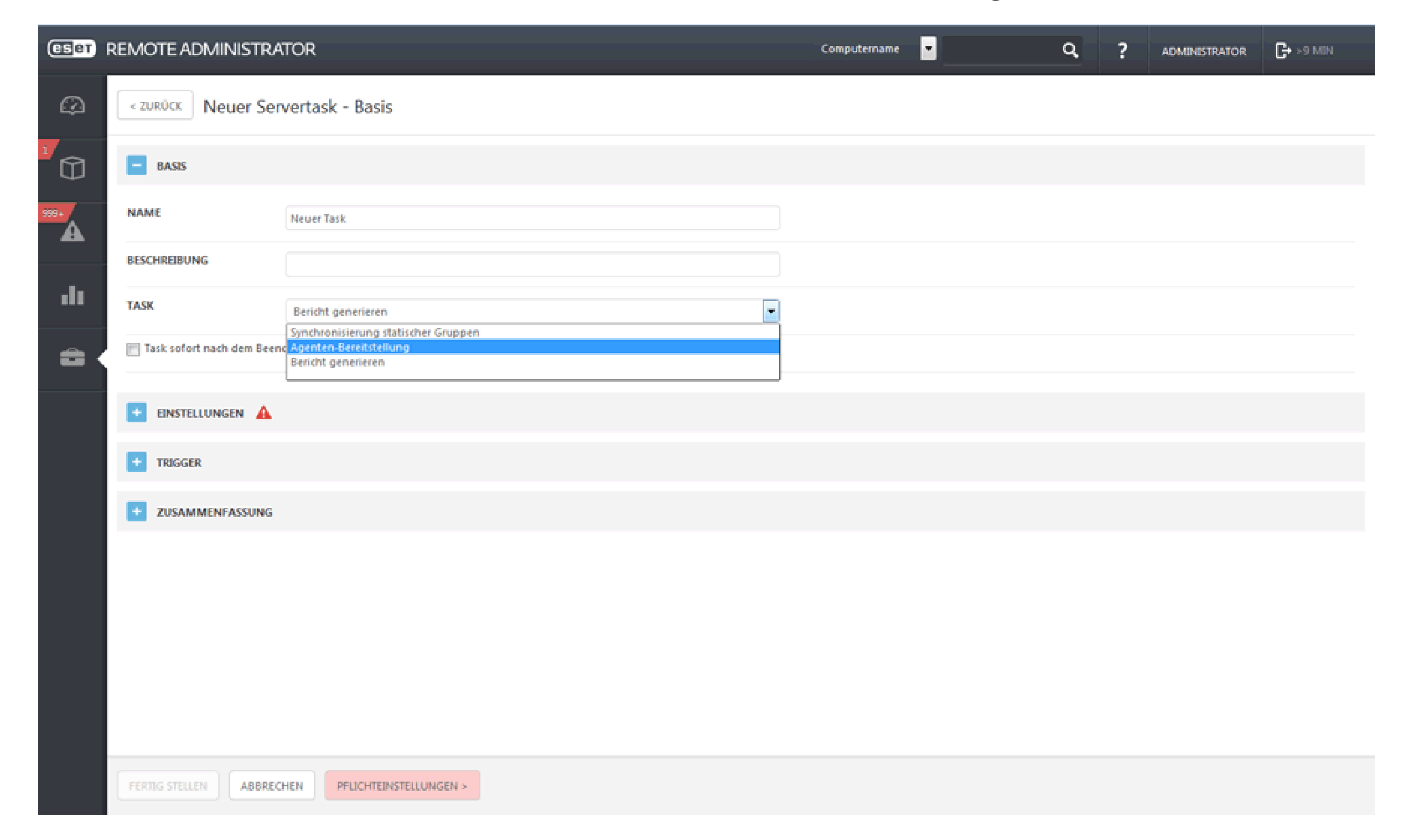
HINWEIS: Testen Sie die massenhafte Agenten-Verteilung nach Möglichkeit zunächst in Ihrer Umgebung. Sobald der Prozess funktioniert, können sie mit der eigentlichen Bereitstellung auf den Clientcomputern der Benutzer beginnen. Außerdem sollten Sie das Verbindungsintervall für Agenten ändern, bevor Sie mit den Tests der massenhaften Bereitstellung beginnen.

Klicken Sie auf **Servertask** > **Agenten-Bereitstellung** > **Neu...**, um mit der Konfiguration des neuen Tasks zu beginnen.



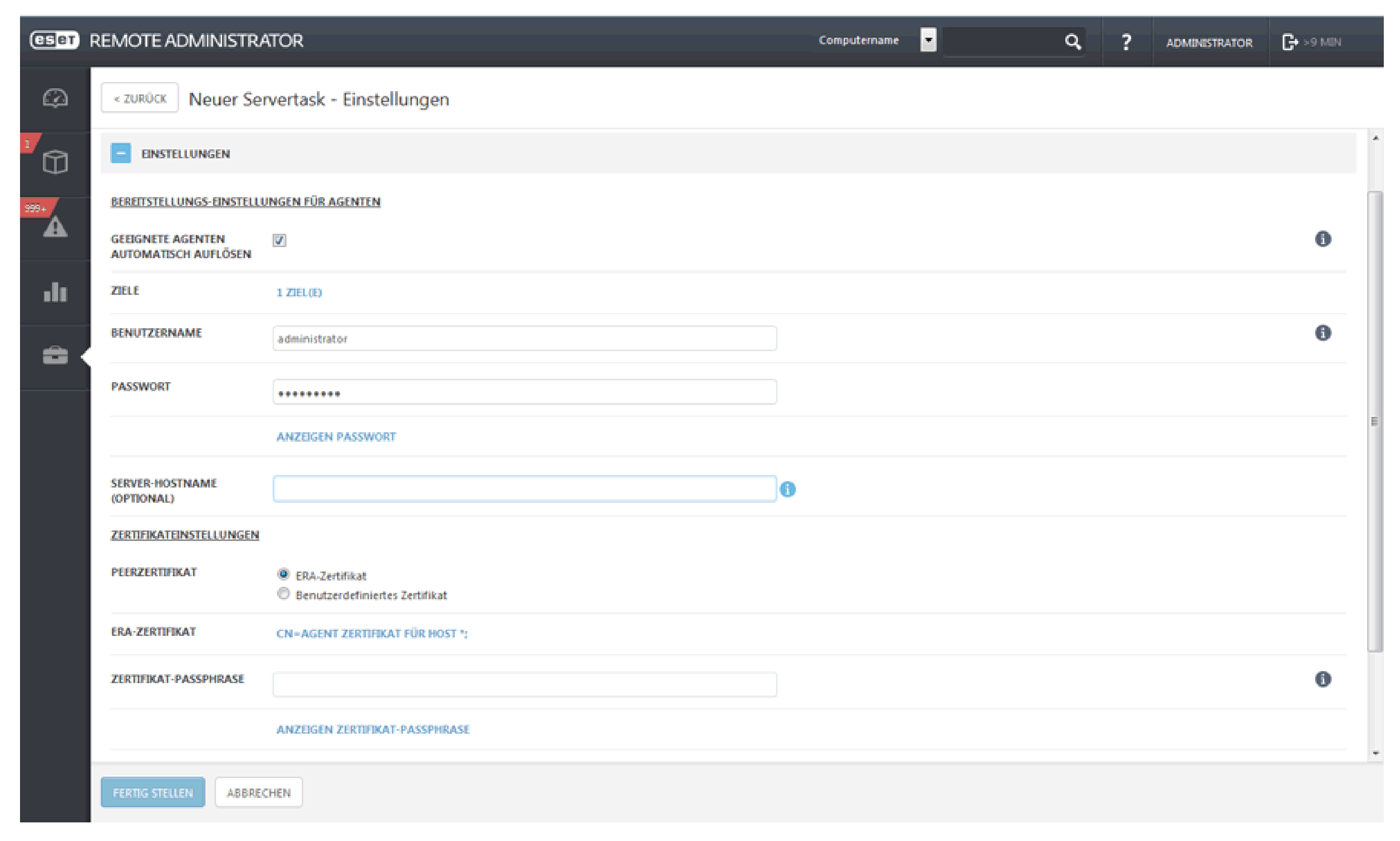
Einfach

Geben Sie grundlegende Informationen zum Task ein, wie **Name**, **Beschreibung** (optional) und **Tasktyp**. Der **Tasktyp** legt die Einstellungen und das Verhalten des Tasks fest. Markieren Sie das Kontrollkästchen neben "Task sofort nach dem Beenden ausführen", um den Task sofort auszuführen, nachdem Sie auf "Fertig stellen" klicken.



Einstellungen

- **Geeignete Agenten automatisch auflösen** – Wenn in Ihrem Netzwerk mehrere Betriebssysteme (Windows, Linux, Mac OS) verwendet werden, wählen Sie diese Option aus, damit der Task für jedes System automatisch das geeignete und serverkompatible Agenten-Installationspaket ermittelt.
- **Ziele** – Klicken Sie auf diese Option, um die Clients auszuwählen, die Empfänger des Task sein sollen.
- **Benutzername/Passwort** – Benutzername und Passwort eines Benutzers mit ausreichenden Rechten zum Ausführen einer Remote-Installation des Agenten.
- **Server-Hostname (optional)** – Hier können Sie einen Server-Hostnamen eingeben, falls auf der Clientseite und der Serverseite unterschiedliche Hostnamen verwendet werden.
- **Peerzertifikat/ERA-Zertifikat** – Sicherheitszertifikat und Zertifizierungsstelle für die Agenten-Installation. Sie können das standardmäßige Zertifikat mit Zertifizierungsstelle auswählen oder benutzerdefinierte Zertifikate verwenden. Weitere Informationen finden Sie im Kapitel Zertifikate.
- **Benutzerdefiniertes Zertifikat** – Wenn Sie ein benutzerdefiniertes Zertifikat für die Authentifizierung verwenden, navigieren Sie während der Installation des Agenten zum Zertifikat und wählen Sie es aus.
- **Zertifikat-Passphrase** – Passwort für das Zertifikat: entweder das Passwort, das Sie während der Serverinstallation (beim Erstellen der Zertifizierungsstelle) eingegeben haben, oder das Passwort Ihres benutzerdefinierten Zertifikats.



HINWEIS: Der ERA-Server kann automatisch das geeignete Agenten-Installationspaket für das entsprechende Betriebssystem ermitteln. Um manuell ein Paket zu wählen, deaktivieren Sie die Option **Geeignete Agenten automatisch auflösen** und wählen Sie über das ERA-Repository das gewünschte Paket aus der Liste der verfügbaren Agenten.

Ziel

Hier können Sie die Clients (einzelne Computer oder ganze Gruppen) festlegen, die Empfänger des Task sein sollen.

Klicken Sie auf **Ziele hinzufügen**, um alle statischen und dynamischen Gruppen und ihre Mitglieder anzuzeigen.

Wählen Sie Clients aus, klicken Sie auf **OK** und fahren Sie mit dem Bereich „Trigger“ fort.

Trigger – Legt fest, welche Ereignisse den Task auslösen.

- **Geplanter Trigger** – Löst den Task zu einem geplanten Zeitpunkt aus. Sie können eine einmalige oder wiederholte Ausführung des Task planen oder zur Planung einen CRON-Ausdruck verwenden.
- **Baldmöglichst** – Der Task wird ausgeführt, sobald der Client eine Verbindung zum ESET Remote Administrator-Server herstellt und den Task empfängt. Wenn der Task nicht vor dem **Ablaufdatum** ausgeführt werden kann, wird er aus der Warteschlange entfernt. Der Task wird nicht gelöscht, aber auch nicht ausgeführt.
- **Ereignislog-Trigger** – Führt den Task beim Eintreten der festgelegten Ereignisse aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Legen Sie den **Logtyp**, den **logischen Operator** und **Filterkriterien** fest, für die der Task ausgelöst werden soll.
- **Trigger bei Aufnahme in dynamische Gruppe** – Dieser Trigger führt den Task aus, wenn ein Client zu der unter „Ziel" ausgewählten dynamischen Gruppe hinzugefügt wird. Wenn eine statische Gruppe oder einzelne Clients ausgewählt wurden, ist diese Option nicht verfügbar.

HINWEIS: Weitere Informationen zu Triggern finden Sie im Kapitel Trigger.

Erweiterte Einstellungen – Drosselung – Die Drosselung schränkt die Ausführung eines Task ein, wenn das auslösende Ereignis sehr oft auftritt, beispielsweise ein **Ereignislog-Trigger** oder **Zusammengeführter dynamischer Gruppen-Trigger** (siehe oben). Weitere Informationen finden Sie im Kapitel Drosselung.

Klicken Sie auf **Fertig stellen**, wenn Sie die Empfänger des Task und die Trigger zum Auslösen des Task definiert haben.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen", wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

Die Agenten-Bereitstellung kann auf verschiedene Weisen erfolgen. Folgende Bereitstellungsmethoden stehen zur Verfügung:

Remote - über einen Servertask für die Massenbereitstellung des ERA-Agenten. Alternativ können Sie den Agenten mithilfe von GPO und SCCM bereitstellen
Lokal - mithilfe des Agenten-Installationspakets oder Live-Installationsprogramms für Agenten, zum Beispiel wenn bei der Remote-Bereitstellung Probleme auftreten

Die lokale Bereitstellung kann auf drei verschiedene Weisen ausgeführt werden:

- Live-Installationsprogramm für Agenten - Unter Verwendung eines generierten Skripts in der ERA Web-Konsole können Sie das Live-Installationsprogramm für Agenten per E-Mail verteilen oder von einem Wechselmedium (z. B. einem USB-Speicher) ausführen
- Servergestützte Installation - unter Verwendung des Agenten-Installationspakets. Die Zertifikate werden automatisch vom ERA-Server heruntergeladen (empfohlen für die lokale Bereitstellung)
- Offline-Installation - mit dem Agenten-Installationspaket. Bei dieser Bereitstellungsmethode müssen Sie die Zertifikate manuell exportieren

Der Task zur Remote-Bereitstellung von Agenten kann zur Massenverteilung von Agenten auf die Clientcomputer verwendet werden. Dies ist die bequemste Verteilungsmethode, da sie von der Web-Konsole aus ausgeführt werden kann und der Agent nicht manuell auf jedem Computer einzeln bereitgestellt werden muss.

Der ERA-Agent ist eine wichtige Komponente, weil die Kommunikation zwischen den ESET-Sicherheitslösungen auf den Clientcomputern und dem ERA-Server ausschließlich über den Agenten erfolgt.

HINWEIS: Wenn bei der Remote-Bereitstellung des ERA-Agenten Probleme auftreten (d. h. der Servertask **Agenten-Bereitstellung** schlägt fehl), beachten Sie die Hinweise unter Fehlerbehebung.

6.1.4.2.2 Bericht generieren

Der Task **Bericht generieren** ermöglicht das Generieren von Berichten über zuvor erstellte oder vordefinierte Bericht-Templates.

Einstellungen

Bericht-Template - Wählen Sie ein Bericht-Template aus der Liste aus.

Wählen Sie E-Mail senden oder In Datei speichern aus, um den generierten Bericht zu erhalten.

E-MAIL SENDEN

Zum Senden/Empfangen von E-Mail-Nachrichten müssen Sie unter Servereinstellungen > „Erweiterte Einstellungen“ die SMTP-Einstellungen konfigurieren.

E-Mail-Nachricht

- **Senden an** - Geben Sie die E-Mail-Adresse(n) der Empfänger für die per E-Mail gesendeten Berichte ein. Trennen Sie mehrere Adressen durch Kommas (,). Sie können auch CC- und BCC-Felder hinzufügen. Diese funktionieren genau wie in E-Mail-Programmen.
- **Betreff** - Betreff für die Nachricht mit dem Bericht. Geben Sie einen klaren Betreff ein, um das Sortieren der eingehenden Nachrichten zu ermöglichen. Dies ist eine optionale Einstellung. Wir empfehlen jedoch, den Betreff nicht leer zu lassen.
- **Nachrichteninhalte** - Definieren Sie den Nachrichtenkörper für die Berichtnachricht.
- **E-Mail senden, wenn Bericht leer ist** - Aktivieren Sie diese Option, wenn der Bericht auch dann gesendet werden soll, wenn er keine Daten enthält.

Druckoptionen

Klicken Sie auf **Druckoptionen anzeigen**, um die folgenden Einstellungen anzuzeigen:

- **Ausgabeformat** – Wählen Sie das geeignete Dateiformat aus. Der erzeugte Bericht wird an die Nachricht angehängt und kann später gedruckt werden.
- **Ausgabesprache** – Wählen Sie die Sprache für die Nachricht aus. Standardmäßig ist die in der ERA Web-Konsole verwendete Sprache ausgewählt.
- **Seitengröße/Auflösung/Seitenausrichtung/Farbformat/Randeinheiten/Ränder** – Diese Optionen sind wichtig, wenn Sie den Bericht drucken möchten. Wählen Sie je nach bevorzugten Druckeinstellungen die gewünschten Optionen aus. Diese Optionen werden nur für die Formate PDF und PS angewendet, nicht für das CSV-Format.

HINWEIS: Für den Task **Bericht generieren** können Sie aus verschiedenen Formaten für die Ausgabedatei auswählen. Wenn Sie das CSV-Format auswählen, werden die Datums- und Uhrzeitwerte des Berichts im UTC-Format gespeichert. Wenn Sie eine der anderen beiden Formate (PDF, PS) auswählen, verwendet der Bericht die örtliche Zeit des Servers.

IN DATEI SPEICHERN

Dateioptionen

- **Relativer Dateipfad** - Der Bericht wird in einem bestimmten Verzeichnis erstellt, zum Beispiel: *C:\Users\All Users\ESET\RemoteAdministrator\Server\Data\GeneratedReports*
- **E-Mail speichern, wenn Bericht leer ist** - Aktivieren Sie diese Option, wenn der Bericht auch dann gespeichert werden soll, wenn er keine Daten enthält.

Druckoptionen

Klicken Sie auf **Druckoptionen anzeigen**, um die folgenden Einstellungen anzuzeigen:

- **Ausgabeformat** – Wählen Sie das geeignete Dateiformat aus. Der erzeugte Bericht wird an die Nachricht angehängt und kann später gedruckt werden.
- **Ausgabesprache** – Wählen Sie die Sprache für die Nachricht aus. Standardmäßig ist die in der ERA Web-Konsole verwendete Sprache ausgewählt.
- **Seitengröße/Auflösung/Seitenausrichtung/Farbformat/Randeinheiten/Ränder** – Diese Optionen sind wichtig, wenn Sie den Bericht drucken möchten. Wählen Sie je nach bevorzugten Druckeinstellungen die gewünschten Optionen aus. Diese Optionen werden nur für die Formate PDF und PS angewendet, nicht für das CSV-Format.

HINWEIS: Für den Task **Bericht generieren** können Sie aus verschiedenen Formaten für die Ausgabedatei auswählen. Wenn Sie das CSV-Format auswählen, werden die Datums- und Uhrzeitwerte des Berichts im UTC-Format gespeichert. Wenn Sie eine der anderen beiden Formate (PDF, PS) auswählen, verwendet der Bericht die örtliche Zeit des Servers.

Trigger

Wählen Sie einen vorhandenen Trigger für den Task aus oder erstellen Sie einen neuen Trigger. Sie können einen ausgewählten Trigger außerdem **Entfernen** oder **Ändern**.

Zusammenfassung

Hier werden alle konfigurierten Optionen angezeigt. Überprüfen Sie die Einstellungen und klicken Sie auf „Fertig stellen“, wenn Sie keine Änderungen mehr vornehmen möchten. Der Task ist jetzt erstellt und kann verwendet werden.

HINWEIS: Für Ubuntu Server Edition müssen **X Server** und **xinit** installiert werden, damit der Berichtdrucker (PDF-Berichte) richtig funktioniert.

```
sudo apt-get install server-xorg
sudo apt-get install xinit
startx
```

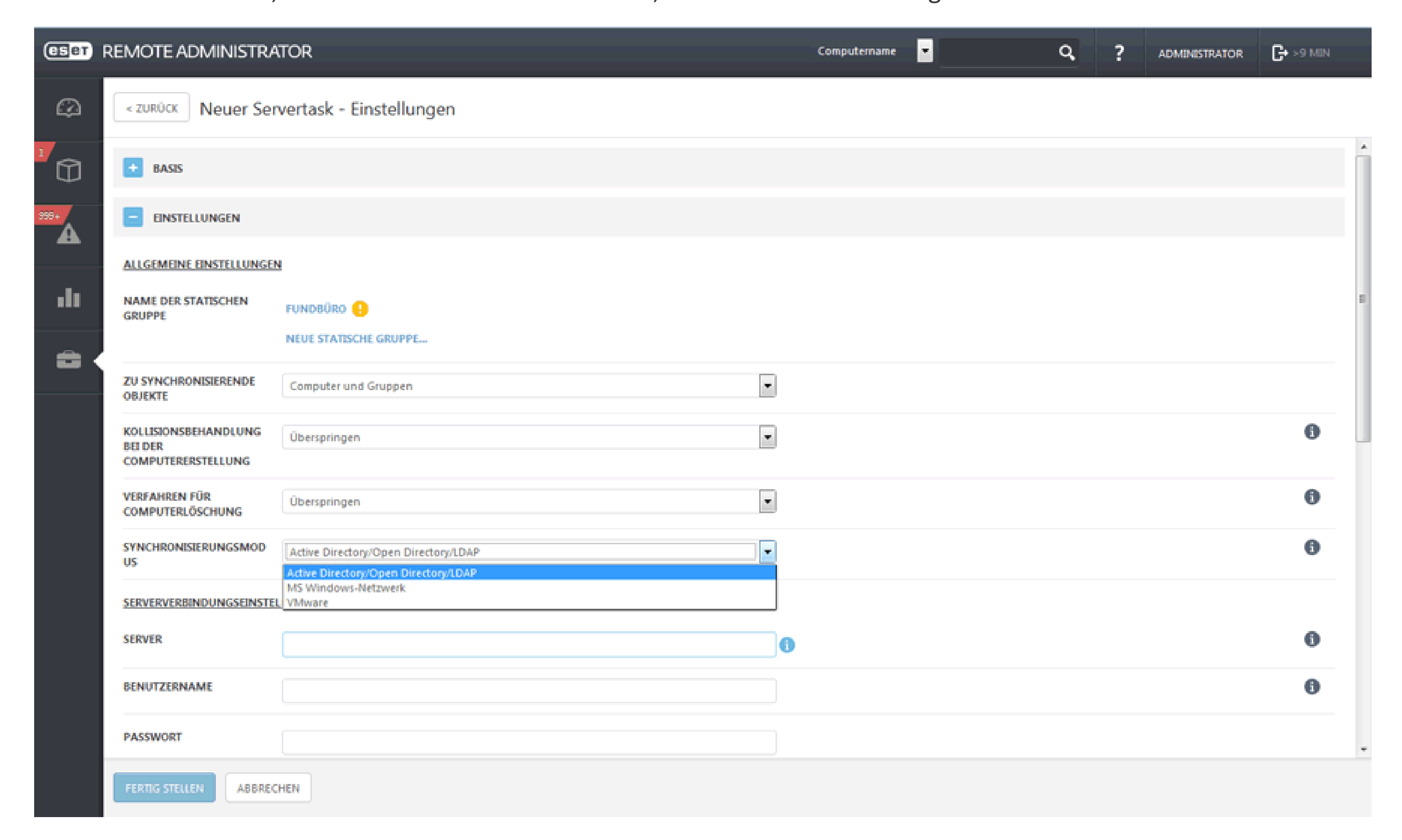
6.1.4.2.3 Synchronisierung statischer Gruppen

Der Task **Synchronisierung statischer Gruppen** durchsucht das Netzwerk (Active Directory, Mac Open Directory, LDAP, lokales Netzwerk) nach Computern und fügt sie in eine statische Gruppe ein. Wenn Sie während der Server-Installation die Option **Mit Active Directory synchronisieren** auswählen, werden die gefundenen Computer zur Gruppe **Alle** hinzugefügt.

Klicken Sie auf **Admin** > **Servertask** > **Synchronisierung statischer Gruppen** > **Neu...**, um mit der Konfiguration des neuen Tasks zu beginnen.

Einfach

Geben Sie grundlegende Informationen zum Task ein, z. B. **Name** und **Beschreibung** (optional). Der **Tasktyp** legt die Einstellungen und das Verhalten des Tasks fest. Markieren Sie das Kontrollkästchen neben "Task sofort nach dem Beenden ausführen", um den Task sofort auszuführen, nachdem Sie auf "Fertig stellen" klicken.



Einstellungen

- **Name der statischen Gruppe** - Diese Gruppe ist der Stamm für die synchronisierten Computer.
- **Zu synchronisierendes Objekt** - Entweder **Computer und Gruppen** oder **Nur Computer**.
- **Kollisionsbehandlung bei der Computererstellung** - Wenn während der Synchronisierung Computer hinzugefügt werden, die bereits Mitglied der statischen Gruppe sind, wird eine Konfliktauflösungsmethode angewendet. Wählen Sie eine Methode aus: Überspringen (die synchronisierten Computer werden nicht hinzugefügt), Verschieben (neue Computer werden in eine Untergruppe verschoben) oder Duplizieren (neue Computer werden mit einem anderen Namen hinzugefügt).
- **Verfahren für Computerlöschung** - Für einen nicht mehr vorhandenen Computer können Sie die Option **Entfernen** oder **Überspringen** auswählen.

Synchronisierungsmodus:

- **Active Directory/Open Directory/LDAP -** Geben Sie die grundlegenden **Serververbindungsinformationen** (Servername, Anmeldename, Passwort) ein.
- **MS Windows-Netzwerk -** Geben Sie eine **Arbeitsgruppe** und den Benutzer mit den Anmeldedaten (Benutzername und Passwort) ein.
- **VMware -** Geben Sie den Hostnamen oder die IP-Adresse und die Anmeldedaten für den Zugriff auf den VMware vCenter-Server ein.

Serververbindungseinstellungen:

- **Server** - Geben Sie den Servernamen oder die IP-Adresse Ihres Domänencontrollers ein.
- **Anmeldung** - Geben Sie die Anmeldeinformationen für Ihren Domänencontroller im Format **Domäne \Benutzername** ein.
- **Passwort** - Geben Sie das Passwort für die Anmeldung bei Ihrem Domänencontroller ein.

- **LDAP-Parameter verwenden -** Falls Sie LDAP verwenden möchten, markieren Sie das Kontrollkästchen **LDAP anstatt Active Directory verwenden** und geben Sie die Attribute für Ihren Server ein. Alternativ können Sie eine **Voreinstellung** auswählen, indem Sie auf **Benutzerdefiniert...** klicken. In diesem Fall werden die Attribute automatisch ausgefüllt.

Synchronisierungseinstellungen:

- **Distinguished Name** - Pfad (Distinguished Name) zum Knoten im Active Directory-Baum. Wenn diese Option leer gelassen wird, wird der gesamte AD-Baum synchronisiert.
- **Ausgeschlossene Distinguished Names** - Wahlweise können Sie bestimmte Knoten im Active Directory-Baum ausschließen (ignorieren).
- **Deaktivierte Computer ignorieren (nur in Active Directory)** - Mit dieser Option können Sie festlegen, ob deaktivierte Computer in Active Directory ignoriert werden sollen. Der Task überspringt diese Computer dann.

Trigger

Wählen Sie einen vorhandenen Trigger für den Task aus oder erstellen Sie einen neuen Trigger. Sie können einen ausgewählten Trigger außerdem **Entfernen** oder **Ändern**.

Zusammenfassung

Überprüfen Sie die angezeigten Konfigurationsinformationen. Wenn Sie keine Änderungen vornehmen möchten, klicken Sie auf **Fertig stellen**. Der Task ist jetzt erstellt und kann verwendet werden.
Nur Windows-Computer sind standardmäßig Empfänger. Wenn die Windows-Domäne Linux-Computer enthält und diese ebenfalls Empfänger des Task sein sollen, machen Sie die Linux-Computer zuerst sichtbar. Für einen Linux-Computer in einer Windows-Domäne wird in den Computereigenschaften unter „Active Directory-Benutzer und -Gruppen“ (ADUC) kein Text angezeigt. Daher muss der Text manuell eingefügt werden.

6.1.4.2.4 Synchronisierung statischer Gruppen - Linux-Computer

Für einen Linux-Computer in einer Windows-Domäne wird in den Computereigenschaften unter „Active Directory-Benutzer und -Gruppen“ (ADUC) kein Text angezeigt. Daher muss der Text manuell eingefügt werden.

- Überprüfen Sie Sie Servervoraussetzungen und die folgenden weiteren Voraussetzungen:

- Die Linux-Computer sind in Active Directory enthalten.
- Der Domänencontroller hat einen installierten DNS-Server.
- **ADSI Edit** ist installiert.

1. Öffnen Sie eine Befehlszeile und führen Sie den folgenden Befehl aus adsiedit.msc
2. Wechseln Sie zu **Aktion** > **Verbinden mit**. Das Fenster für die Verbindungeinstellungen wird angezeigt.
3. Klicken Sie auf **Einen allgemein bekannten Namenskontext auswählen**.
4. Erweitern Sie das Kombinationsfeld und wählen Sie den Namenskontext **Standard** aus.
5. Klicken Sie auf **OK**. Der ADSI-Wert links sollte der Name Ihres Domänencontrollers ein. Standard-Namenskontext (Ihr Domänencontroller).
6. Klicken Sie auf den **ADSI**-Wert und erweitern Sie die Untergruppe.
7. Klicken Sie auf die **Untergruppe** und navigieren Sie zum CN (Common Name) oder zur OU (Organizational Unit), wo die Linux-Computer angezeigt werden.
8. Klicken Sie auf den **Hostnamen** des Linux-Computers und wählen Sie **Eigenschaften** aus dem Kontextmenü aus. Navigieren Sie zum Parameter **dNSHostName** und klicken Sie auf **Bearbeiten**.
9. Ändern Sie den Wert **<nicht festgelegt>** in einen gültigen Text (zum Beispiel *ubuntu.TEST*).
10. Klicken Sie auf **OK** > **OK** Öffnen Sie **ADUC** und wählen Sie die **Eigenschaften** des Linux-Computers aus. Der neue Text sollte angezeigt werden.

6.1.4.3 Planen eines Server-Tasks

Ein geplanter Trigger führt den Task gemäß den Datums- und Uhrzeiteinstellungen aus. Für den Task kann eine **einmalige** oder wiederholte Ausführung oder eine Ausführung gemäß CRON-Ausdruck geplant werden.

6.1.4.4 Trigger in Servertask wiederverwenden

Das Wiederverwenden eines Triggers bedeutet, dass ein bestimmter Trigger (Umstand/Ereignis) mehrere Tasks (Aktionen) gleichzeitig initiieren kann.

Beispiel: Ein ERA-Benutzer möchte gleichzeitig zwei unterschiedliche monatliche Berichte erstellen. Führen Sie die unten genannten Schritte aus, um den Trigger des ersten Berichts zum Erstellen des zweiten Berichts wiederzuverwenden.

1. Erstellen Sie den ersten Berichtgenerierungstask mit einem zugewiesenen, monatlich geplanten Trigger.
2. Beginnen Sie mit der Konfiguration des zweiten Berichtgenerierungstasks mit einem anderen Bericht.
3. Klicken Sie im Bildschirm „Trigger“ des Taskerstellungsassistenten auf **Bestehende hinzufügen ...**. Die Liste der vorhandenen Trigger wird angezeigt.
4. Wählen Sie den gleichen Trigger mit monatlicher Planung aus, der auch für den ersten Berichterstellungstask verwendet wurde.
5. **Speichern** Sie den Task. Wenn diese Schritte ausgeführt wurden, werden jeden Monate gleichzeitig zwei verschiedene Berichte generiert.

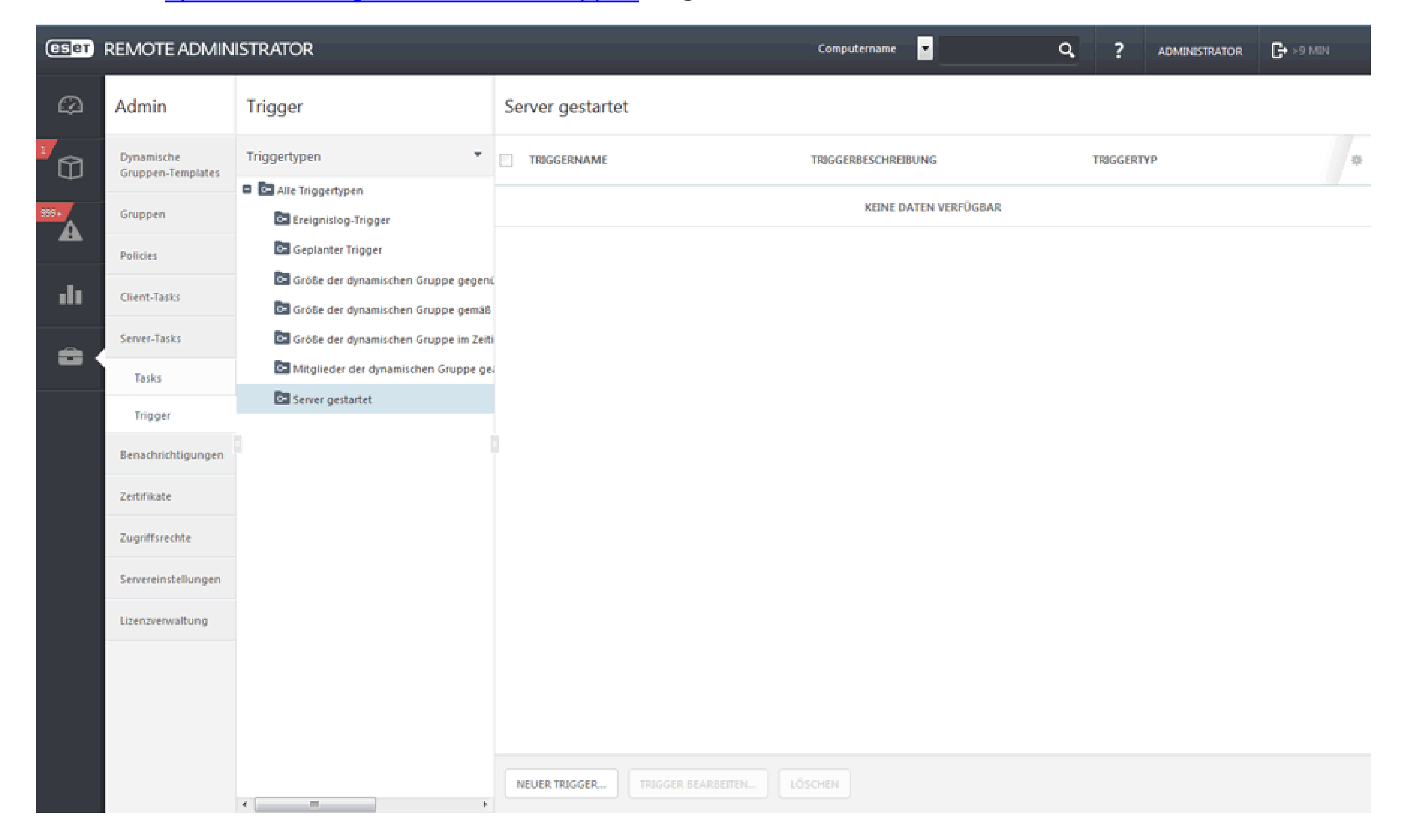
6.1.4.5 Trigger

Trigger sind „Sensoren“, die auf eine vordefinierte Weise auf bestimmte Ereignisse reagieren. Sie werden eingesetzt, um eine Aktion (in den meisten Fällen einen Task) auszuführen. Sie können über einen Zeitplan (Zeitereignisse) oder das Auftreten eines bestimmten Systemereignisses aktiviert werden.

Ein Trigger führt alle dem Trigger zugewiesenen Tasks aus, wenn er aktiviert wird. Neu zugewiesene Tasks werden vom Trigger nicht sofort ausgeführt, sondern erst, wenn der Trigger aktiviert wird. Die Triggerempfindlichkeit auf Ereignisse kann durch die Drosselung reduziert werden.

Servertriggertypen:

- **Mitglieder der dynamischen Gruppe geändert -** Dieser Trigger wird aktiviert, wenn die Mitglieder einer dynamischen Gruppe geändert werden. Beispiel: Clients treten der dynamischen Gruppe *Infiziert* bei oder werden aus dieser Gruppe entfernt.
- **Größe der dynamischen Gruppe gegenüber Vergleichsgruppe geändert -** Dieser Trigger wird aktiviert, wenn die Anzahl der Clients in einer beobachteten dynamischen Gruppe sich gegenüber einer (statischen oder dynamischen) Vergleichsgruppe ändert. Beispiel: Mehr als 10 % aller Computer sind infiziert (Größe der Gruppe „Alle“ in Bezug auf die Gruppe „Infiziert“).
- **Größe der dynamischen Gruppe gemäß Schwellenwert geändert -** Dieser Trigger wird aktiviert, wenn die Anzahl der Clients in einer dynamischen Gruppe einen festgelegten Schwellenwert über- oder unterschreitet. Beispiel: Mehr als 100 Computer befinden sich in der Gruppe „Infiziert“.
- **Größe der dynamischen Gruppe im Zeitintervall geändert -** Dieser Trigger wird aktiviert, wenn die Anzahl der Clients in einer dynamischen Gruppe sich innerhalb eines bestimmten Zeitintervalls ändert. Beispiel: Die Anzahl der Computer in der Gruppe „Infiziert“ steigt innerhalb einer Stunde um 10 %.
- **Ereignislog-Trigger -** Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt. Beispiel: Im Scan-Log wird eine Bedrohung aufgezeichnet.
- **Geplanter Trigger -**Ein geplanter Trigger wird zu einer bestimmten Uhrzeit/einem bestimmten Datum ausgelöst.
- **Server gestartet -** Dieser Trigger wird beim Starten des Servers aktiviert. Dieser Trigger wird beispielsweise für den Task Synchronisierung der statischen Gruppen eingesetzt.



6.1.4.5.1 Drosselung

Unter bestimmten Umständen kann die Drosselung verhindern, dass ein Trigger ausgelöst wird. Zeitbasierte Bedingungen haben eine höhere Priorität als statistische Bedingungen.

Wenn eine der Bedingungen erfüllt wird, wird die gesamte Statusinformation für alle Beobachter zurückgesetzt (die Beobachtung wird wieder neu begonnen). Dies gilt für zeitbasierte und für statistische Bedingungen. Statusinformationen für Beobachter sind nicht dauerhaft. Sie werden auch zurückgesetzt, wenn der Agent oder der Server neu gestartet werden.

Änderungen an einem Trigger führen zum Zurücksetzen des Triggerstatus.

Die Triggerauslösung kann auf verschiedene Weisen gesteuert werden:

Statistische

Statistische Trigger können durch eine beliebige Kombination der folgenden Parameter ausgelöst werden:

- S1: Der Trigger wird alle **N** Vorkommnisse des Triggerereignisses aktiviert (Modulo-**N**), ausgehend vom letzten Ereignis in einer Serie (beispielsweise N. Ereignis seit dem Start).
- S2: Der Trigger wird aktiviert, wenn **N** Ereignisse innerhalb der Zeit **X** auftreten (das Zeitintervall kann aus einem vordefinierten Satz gewählt werden) [**N** <= 100]. Dabei wird die gleitende Summe betrachtet, d. h. es wird nur die Anzahl der Ereignisse innerhalb des letzten Zeitraums X berücksichtigt. Beim Auslösen des Triggers wird der Puffer zurückgesetzt.
- S3: **N** Ereignisse mit dem eindeutigen Symbol **S** [N <= 100] treten nacheinander auf. Der Puffer wird zurückgesetzt, wenn der Trigger aktiviert wird und im Puffer bereits ein Ereignis vorhanden ist. Der Puffer wird als „gleitendes Fenster“ betrachtet (FIFO-Prinzip). Das neue Symbol wird mit allen Symbolen im Puffer verglichen.
  Hinweis: Ein fehlender Wert (n/a) wird als nicht eindeutig betrachtet und der Puffer daher in diesem Fall seit dem letzten Auslösen zurückgesetzt.

Diese Bedingungen können mit dem Operator AND (alle Bedingungen müssen erfüllt werden) oder OR (eine beliebige Bedingung muss erfüllt werden) kombiniert werden.

Zeitbasiert

Alle folgenden Bedingungen müssen gleichzeitig erfüllt werden (sofern festgelegt):

- T1: Der Trigger wird im Zeitraum **X** ausgeführt. Der Zeitraum wird als wiederholte Serie von Zeitgrenzwerten festgelegt (zum Beispiel zwischen 13:00 und 14:00 ODER 17:00 und 23:30 Uhr).
- T2: Der Trigger kann höchstens alle **X Zeiteinheiten** ausgeführt werden.

Zusätzliche Eigenschaften

Wie bereits erwähnt, löst nicht jedes Ereignis eine Triggeraktivierung aus. Mögliche Aktionen für Ereignisse, die keinen Trigger aktivieren, sind Folgende:

- Wenn mehr als ein Ereignis übersprungen wird, die letzten **N** Ereignisse in einem Ereignis zusammenfassen (Daten unterdrückter Treffer speichern) [**N** <= 100].
- Bei **N** == 0 nur das letzte Ereignis verarbeiten (**N** bedeutet die Verlaufslänge; das letzte Ereignis wird immer verarbeitet).
- Alle Ereignisse, die keinen Trigger aktivieren, zusammenführen (den letzten Treffer mit **N** verstrichenen Treffern zusammenführen).

Beispiele:

S1: Kriterium für Vorkommnisse (jeden 3. Treffer zulassen)

Zeit	00	01	02	03	04	05	06	Trigger wird geändert	07	08	09	10	11	12	13	14	15
Treffer	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: Kriterium für Vorkommnisse innerhalb des Zeitraums (zulassen, wenn 3 Treffer innerhalb von 4 Sekunden auftreten)

Zeit	00	01	02	03	04	05	06	Trigger wird geändert	07	08	09	10	11	12	13
Treffer	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Kriterium für eindeutige Symbolwerte (zulassen, wenn 3 eindeutige Werte in einer Zeile vorhanden sind)

Zeit	00	01	02	03	04	05	06	Trigger wird geändert	07	08	09	10	11	12	13
Wert	A	B	B	C	D	G	H		J	K	nicht verfügbar	L	M	N	N
S3					1									1	

S3: Kriterium für eindeutige Symbolwerte (zulassen, wenn 3 eindeutige Werte seit dem letzten Treffer)

Zeit	00	01	02	03	04	05	06	07	Trigger wird geändert	08	09	10	11	12	13	14
Wert	A	B	B	C	D	G	H	I		J	K	nicht verfügbar	L	M	N	N
S3				1			1						1			

T1: Einen Treffer in einem bestimmten Zeitraum zulassen (täglich ab 8:10 Uhr zulassen, Dauer: 60 Sekunden)

Zeit	08:09:50	08:09:59	08:10:00	08:10:01	Trigger wird geändert	08:10:59	08:11:00	08:11:01
Treffer	x	x	x	x		x	x	x
T1			1	1		1		

Dieses Kriterium hat keinen Status. Änderungen des Triggers haben daher keinen Einfluss auf das Ergebnis.

T2: Einen einzigen Treffer innerhalb eines Zeitintervalls zulassen (höchstens einmal alle 5 Sekunden)

Zeit	00	01	02	03	04	05	06	Trigger wird geändert	07	08	09	10	11	12	13

Treffer	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Kombination aus S1 und S2

- S1: jeder 5. Treffer
- S2: 3 Treffer innerhalb von 4 Sekunden

Zeit	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Treffer	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Ergebnis			1				1								1		

Das Ergebnis wird aufgezählt als: S1 (logisch „oder“) S2

Kombination aus S1 und T1

- S1: Jeden 3. Treffer zulassen
- T1: Täglich ab 8:08 Uhr zulassen, für eine Dauer von 60 Sekunden

Uhrzeit:	08:07:50	08:07:51	08:07:52	08:07:53	08:08:10	08:08:11	08:08:19	08:08:54	08:08:55	08:09:01
Treffer	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
Ergebnis						1			1	

Das Ergebnis wird aufgezählt als: S1 (logisch „und“) T1

Kombination aus S2 und T1

- S2: 3 Treffer innerhalb von 10 Sekunden
- T1: Täglich ab 8:08 Uhr zulassen, für eine Dauer von 60 Sekunden

Uhrzeit:	08:07:50	08:07:51	08:07:52	08:07:53	08:08:10	08:08:11	08:08:19	08:08:54	08:08:55	08:09:01
Treffer	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Ergebnis							1			

Das Ergebnis wird aufgezählt als: S2 (logisch „und“) T1.
Beachten Sie, dass der Status von S2 nur zurückgesetzt wird, wenn das globale Ergebnis „1“ ist.

Kombination aus S2 und T2

- S2: 3 Treffer innerhalb von 10 Sekunden
- T2: Höchstens einmal alle 20 Sekunden zulassen

Uhrzeit:	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Treffer	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
Ergebnis			1													1		

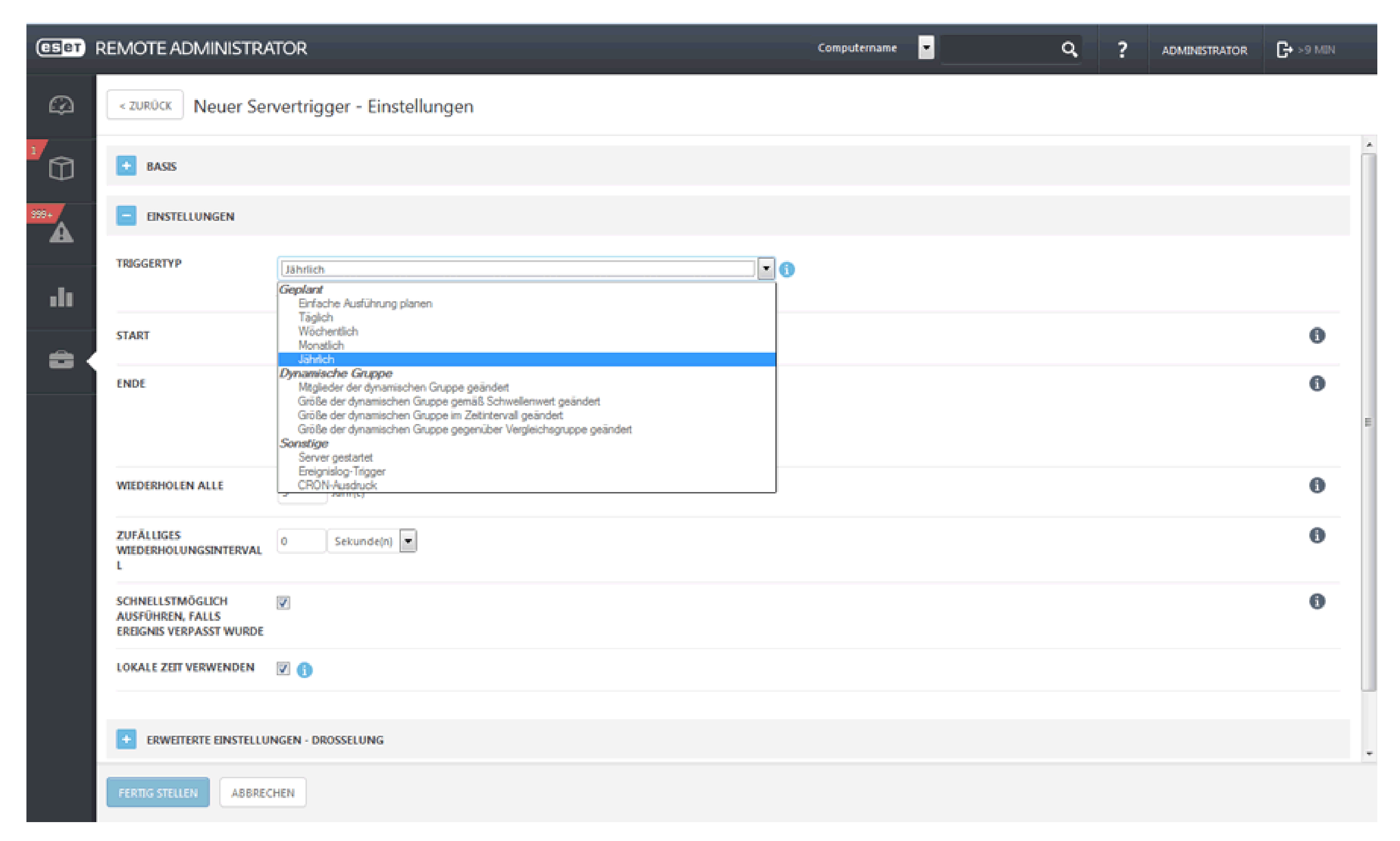
Das Ergebnis wird aufgezählt als: S2 (logisch „und“) T2.
Beachten Sie, dass der Status von S2 nur zurückgesetzt wird, wenn das globale Ergebnis „1“ ist.

6.1.4.5.1.1 Trigger ist zu empfindlich

Verwenden Sie die Drosselungsbedingungen, die im Abschnitt Trigger löst zu oft aus dieses Handbuchs beschrieben sind.

6.1.4.5.2 Assistent für Servertrigger

Trigger werden auf der Registerkarte **Admin** unter **Server-Tasks** > **Triggers** verwaltet. Wählen Sie **Triggertyp** > **Neuer Trigger** aus.



6.1.4.5.3 Verwalten von Servertriggern

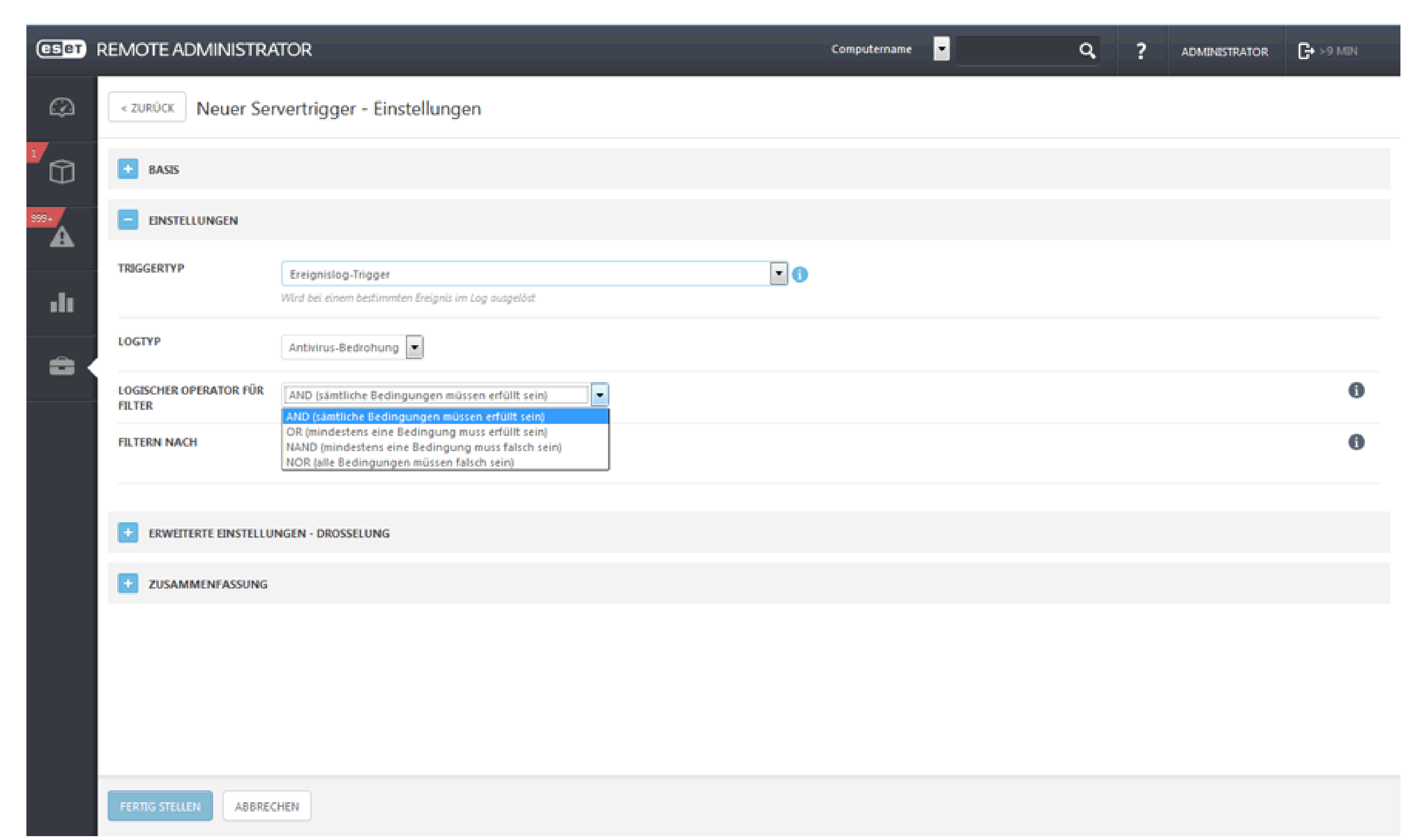
Klicken Sie zum Verwalten der Servertrigger auf der Registerkarte **Admin** auf **Server-Tasks** > **Trigger**. Wählen Sie **Triggertyp** aus und klicken Sie auf **Bearbeiten**.

Basis

Definieren Sie einen **Namen** für den Trigger. Sie können auch eine **Beschreibung** für den Trigger eingeben.

Einstellungen

- Wählen Sie einen Triggertyp aus. Der Triggertyp legt fest, wie der Trigger aktiviert wird. Wählen Sie einen **Ereignislog-Trigger** aus und klicken Sie auf „Weiter“.
- Wählen Sie einen **Logtyp** aus. Der Trigger wird aufgerufen, wenn ein bestimmtes Ereignis in den Logs auftritt.
- Definieren Sie das Ereignis, bei dessen Auftreten der Trigger aktiviert werden soll. Wählen Sie einen **logischen Operator** zum Filtern der Ereignisse aus. Wählen Sie in diesem Beispiel **AND (alle Bedingungen müssen erfüllt werden)** aus.
- Fügen Sie ggf. einen **Filter** aus der Liste (ein Ereignis) hinzu und wählen Sie den logischen Operator für die benutzerdefinierte Zeichenfolge.

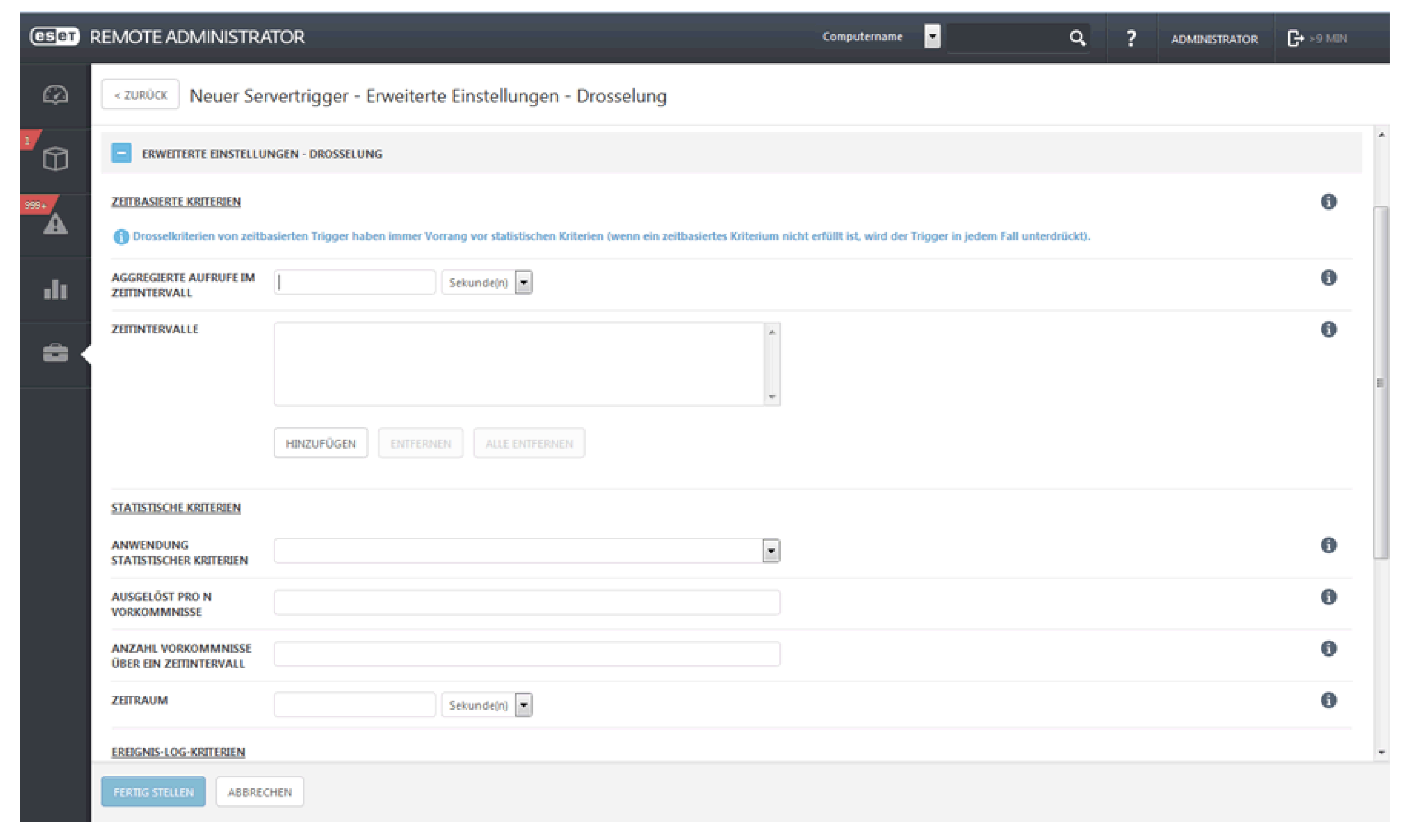


Wählen Sie einen logischen Operator im Menü **Operation** aus.

- **AND** – Alle festgelegten Bedingungen müssen erfüllt sein.
- **OR** – Mindestens eine Bedingung muss erfüllt sein.
- **NAND** – Mindestens eine Bedingung darf nicht erfüllt sein.
- **NOR** – Alle Bedingungen müssen falsch sein.

Erweiterte Einstellungen - Drosselung

Geben Sie die **Anzahl zu aggregierender Ticks** an. Dies legt fest, wie viele Triggertreffer benötigt werden, um den Trigger zu aktivieren. Weitere Informationen finden Sie im Kapitel Drosselung.



Zusammenfassung

Überprüfen Sie die Einstellungen für den neuen Trigger, nehmen Sie je Bedarf Änderungen vor und klicken Sie auf **Fertig stellen**. Der Trigger ist jetzt auf dem Server gespeichert und bereit zur Verwendung. In der Liste rechts können Sie Trigger anzeigen, die Sie erstellt haben. Um einen Trigger zu bearbeiten oder zu löschen, klicken Sie in der Liste auf den Trigger und wählen Sie aus dem Kontextmenü die gewünschte Aktion aus. Um gleichzeitig mehrer Trigger zu löschen, aktivieren Sie die Kontrollkästchen neben den zu entfernenden Triggern und klicken Sie auf **Löschen**.

6.1.4.5.3.1 Trigger löst zu oft aus

Wenn Sie weniger Benachrichtigungen erhalten möchten, beachten Sie folgende Möglichkeiten:

- Wenn eine Benachrichtigung nicht für jedes einzelne Ereignis, sondern nur bei mehreren Ereignissen ausgelöst werden soll, definieren Sie eine statistische Bedingung S1 für die Drosselung.
- Wenn der Trigger nur nach einer Gruppe von Ereignissen ausgelöst werden soll, verwenden Sie die statistische Bedingung S2 der Drosselung.
- Wenn Ereignisse mit unerwünschten Werten ignoriert werden sollen, definieren Sie die statistische Bedingung S3 der Drosselung.
- Wenn Ereignisse außerhalb eines bestimmten Zeitfensters (beispielsweise außerhalb der Arbeitszeiten) ignoriert werden sollen, definieren Sie eine zeitbasierte Bedingung T1 für die Drosselung.
- Um ein Mindestintervall zwischen den Triggeraktivierungen festzulegen, verwenden Sie die zeitbasierte Bedingung T2 der Drosselung.

HINWEIS: Diese Bedingungen können auch kombiniert werden, um eine komplexere Drosselung zu definieren.

6.1.4.5.3.2 CRON-Ausdruck

Mit CRON-Ausdrücken können bestimmte Instanzen eines Triggers definiert werden. Ein CRON-Ausdruck ist eine Zeichenfolge aus 7 Unterausdrücken (Feldern), die Werte für den Zeitplan enthalten. Die Felder sind durch ein Leerzeichen getrennt und können einen beliebigen zulässigen Wert in verschiedenen Kombinationen enthalten.

Name	Erforderlich	Wert	Zulässige Sonderzeichen
Sekunden	Ja	0-59	,-*/
Minuten	Ja	0-59	,-*/
Stunden	Ja	0-23	,-*/
Tag des Monats	Ja	1-31	,-*/ L W C
Monat	Ja	0–11 oder JAN-DEC	,-*/
Wochentag	Ja	1–7 oder SUN-SAT	,-*/ L C #
Jahr	Nein	leer oder 1970–2099	,-*/

Beispiele finden Sie hier.

6.1.4.5.4 Verwalten der Triggerempfindlichkeit

Mithilfe der Drosselung kann das Ausführen eines Tasks eingeschränkt werden, falls der Task durch ein häufig auftretendes Ereignis ausgelöst wird. Unter bestimmten Umständen kann die Drosselung verhindern, dass ein Trigger ausgelöst wird. Wenn eine der definierten Bedingungen erfüllt wird, wird die angehäufte Information für alle Beobachter zurückgesetzt (der Zähler startet erneut bei 0). Diese Informationen werden auch zurückgesetzt, wenn der Agent oder der ERA-Server neu gestartet werden. Alle Änderungen an einem Trigger führen zum Zurücksetzen des Triggerstatus.

Die zeitbasierten Drosselungsbedingungen haben eine höhere Priorität als die statistischen Bedingungen. Es empfiehlt sich, nur eine statistische Bedingung und mehrere zeitbasierte Bedingungen zu verwenden. Mehrere statistische Bedingung stellen unter Umständen eine unnötige Komplikation dar und können das Ergebnis beeinträchtigen.

- **Statistische Bedingungen**

Die statistischen Bedingungen können mit dem logischen Operator **AND** (alle Bedingungen müssen erfüllt werden) oder mit dem logischen Operator **OR** (die erste erfüllte Bedingung löst den Trigger aus) kombiniert werden.

- **Zeitbasierte Bedingungen**

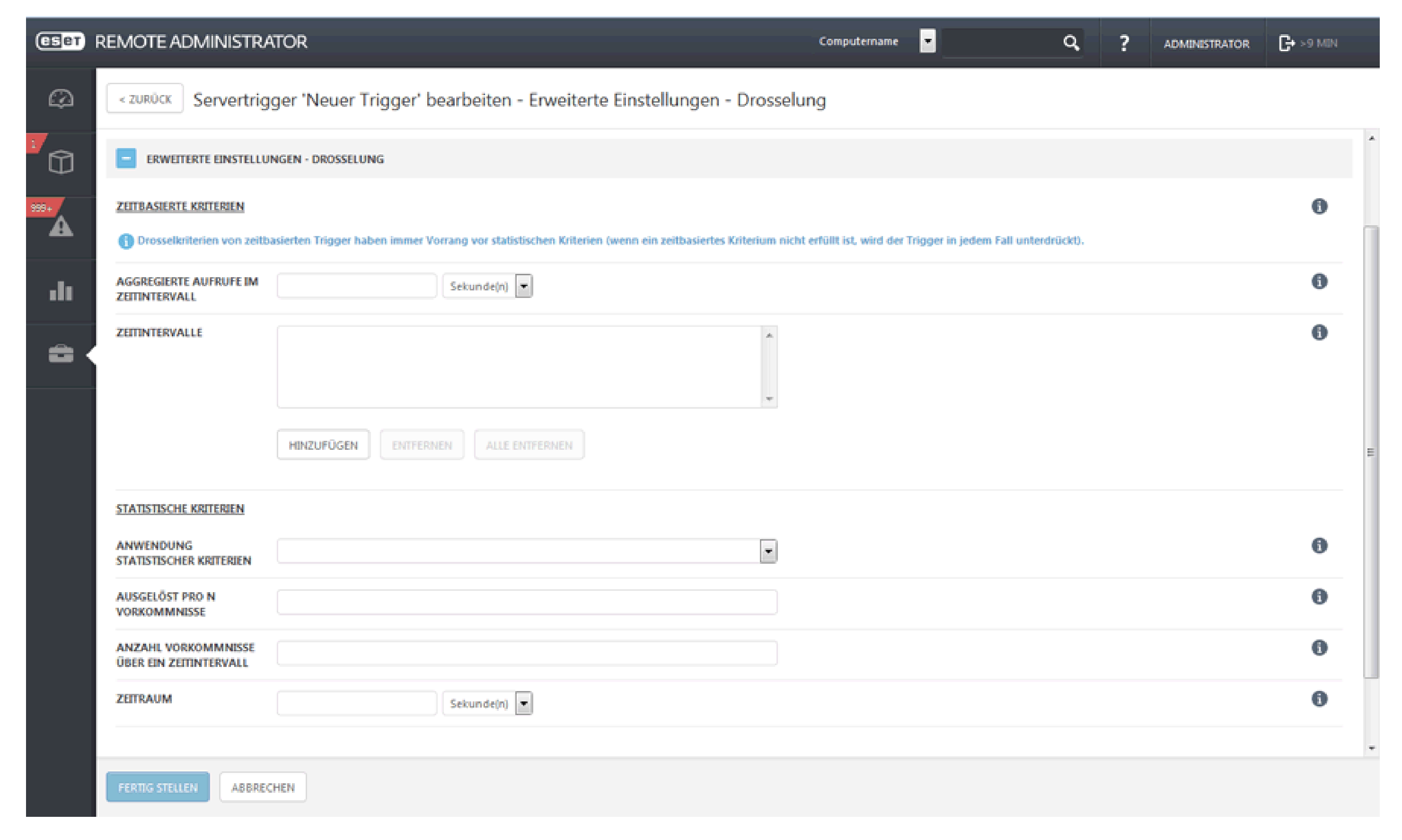
Alle konfigurierten Bedingungen müssen erfüllt sein, um ein Ereignis auszulösen. Die Drosselungskriterien beziehen sich auf die Zeit, zu der das Ereignis eingetreten ist.

Aggregation

- **Anzahl zu aggregierender Ticks** - Anzahl der Treffer (wie oft die Triggerbedingungen erfüllt werden) bis zum Aktivieren des Triggers. Der Trigger wird erst aktiviert, wenn diese Zahl erreicht wurde. Wenn Sie den Wert beispielsweise auf „100“ festlegen, erhalten Sie bei 100 erkannten Bedrohungen nicht 100 Benachrichtigungen, sondern nur eine Benachrichtigung, die auf 100 Bedrohungen hinweist. Wenn 200 Bedrohungen erkannt werden, enthält die Benachrichtigung nur die letzten 100 Bedrohungen.

Zeitbasierte Kriterien

- **Aggregierte Aufrufe über Zeitintervall [s]** - Sie können einen Treffer je x Sekunden zulassen. Wenn Sie diese Option auf 10 Sekunden festlegen und innerhalb dieses Zeitraums 10 Treffer auftreten, wird nur 1 Treffer gezählt.
- **Zeitintervalle** - Mit dieser Option können Sie Treffer nur innerhalb eines definierten Zeitintervalls zulassen. Die Liste kann mehrere Zeitintervalle enthalten, die dann chronologisch geordnet sind.



Statistische Kriterien

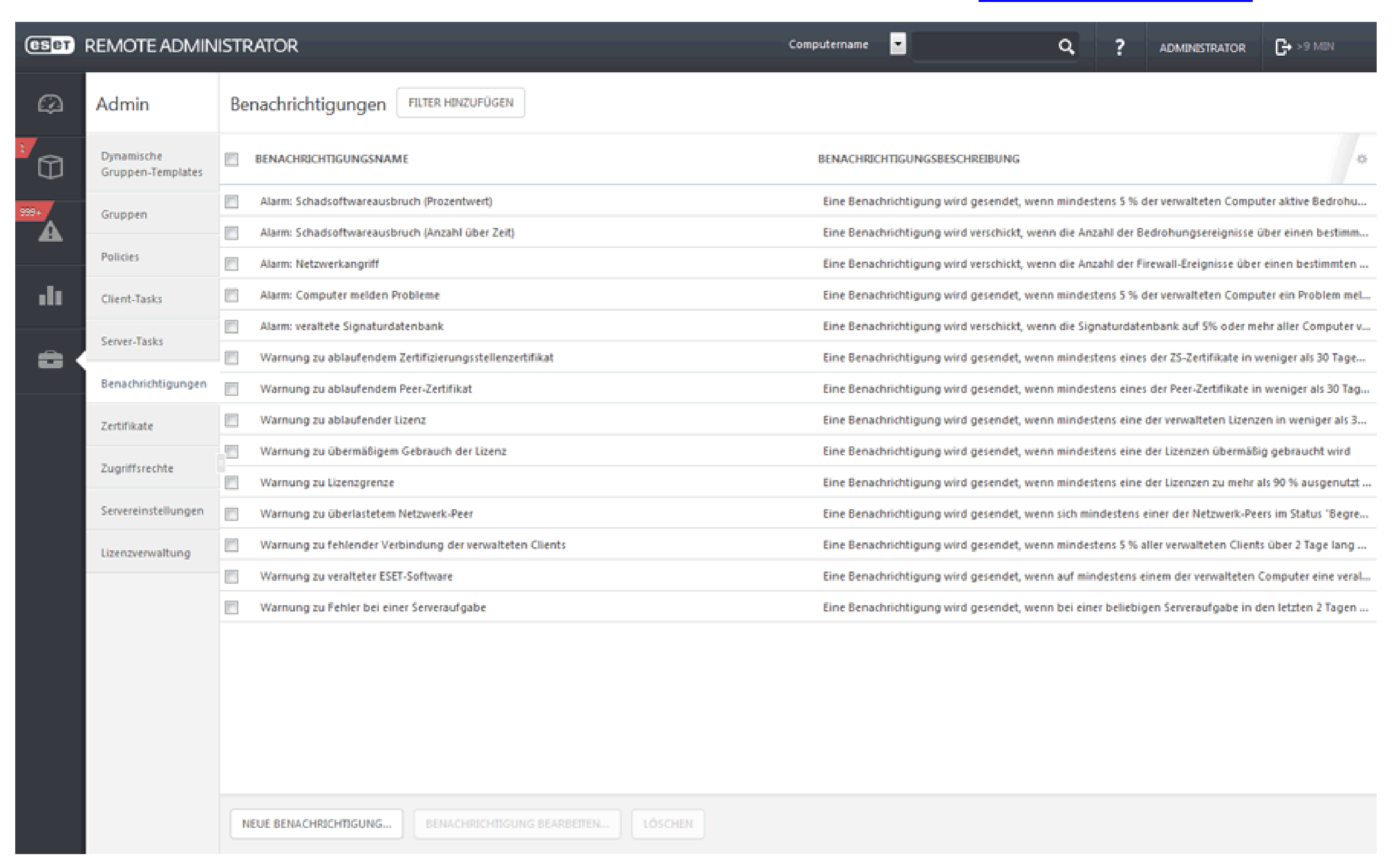
- **Anwendung statistischer Kriterien** - Diese Option legt fest, mit welcher Methode die statistischen Kriterien bewertet werden. Es müssen entweder alle Kriterien (**UND**) oder mindestens ein Kriterium (**ODER**) erfüllt werden.
- **Ausgelöst je Anzahl Vorkommnisse** - Nur jeden **X.** Treffer zulassen. Wenn Sie beispielsweise „10“ eingeben, wird nur jeder 10. Treffer gezählt.
- **Anzahl Vorkommnisse über ein Zeitintervall** - Nur Treffer im definierten Zeitintervall zulassen. Diese Option legt die Frequenz fest. Sie können beispielsweise festlegen, dass der Task ausgeführt wird, wenn das Ereignis innerhalb von einer Stunde 10 Mal auftritt.
  - **Zeitraum** - Definieren Sie hier den Zeitraum für die oben beschriebene Option.
- **Anzahl Ereignisse mit Symbol** - Treffer aufzeichnen, wenn **X** Ereignisse mit dem angegebenen Symbol eingetreten sind. Wenn Sie beispielsweise „10“ eingeben, wird ein Treffer je 10 Installationen einer bestimmten Anwendung gezählt.
  - Gilt für Anzahl von Ereignissen - Geben Sie an, nach wie vielen aufeinanderfolgenden Ereignissen nach dem letzten Treffer ein weiterer Treffer gezählt werden soll. Wenn Sie beispielsweise „10“ eingeben, wird 10 Ereignisse nach dem letzten Treffer ein neuer Treffer gezählt.

- **Gilt für Anzahl von Ereignissen** - Sie können festlegen, ob zur Anwendung des Triggers die in Serie empfangenen Treffer (**Empfangen in Serie**; die Triggerausführung wird nicht berücksichtigt) oder die Treffer seit der letzten Triggerausführung (**Empfangen seit letzter Triggerausführung**, d. h. beim Ausführen des Triggers wird der Zähler auf 0 zurückgesetzt) berücksichtigt werden.

6.1.5 Benachrichtigungen

Benachrichtigungen sind wichtig, um den Gesamtstatus im Netzwerk zu beobachten. Wenn ein neues Ereignis eintritt (je nach Konfiguration), werden Sie mit einer festgelegten Methode (SNMP-Trap oder E-Mail-Nachricht) benachrichtigt und können entsprechend reagieren.

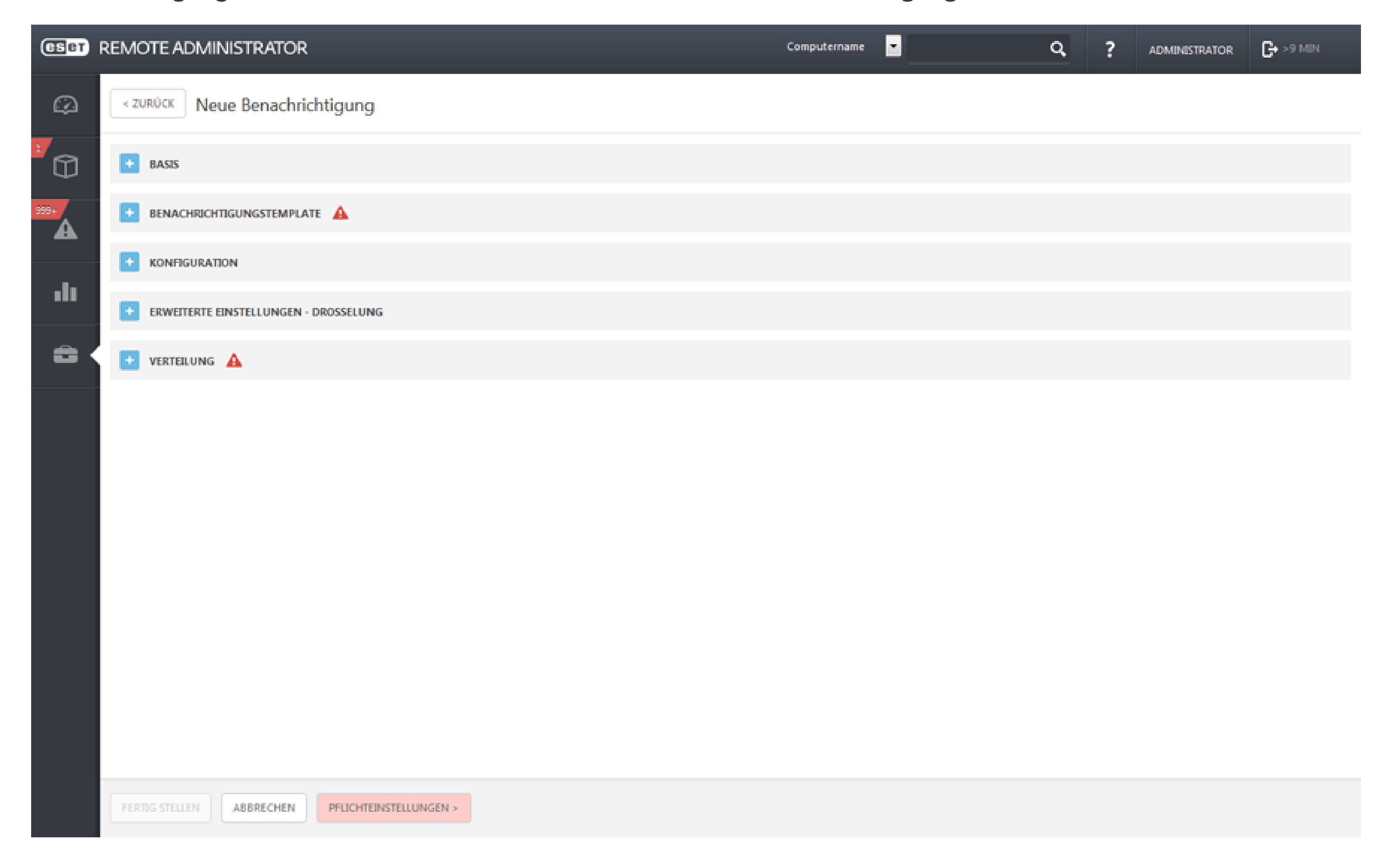
- Alle Benachrichtigungstemplates werden in der Liste angezeigt. Sie können die Templates nach **Name** oder **Beschreibung** filtern.
- Klicken Sie auf **Filter hinzufügen**, um Filterkriterien hinzuzufügen und/oder eine Zeichenfolge in das Feld **Name** oder **Benachrichtigung** einzugeben.
- Wenn Sie eine vorhandene Benachrichtigung auswählen, stehen die Funktionen **Bearbeiten** und **Löschen** zur Verfügung.
- Um eine neue Benachrichtigung zu erstellen, klicken Sie unten auf der Seite auf Neue Benachrichtigung.



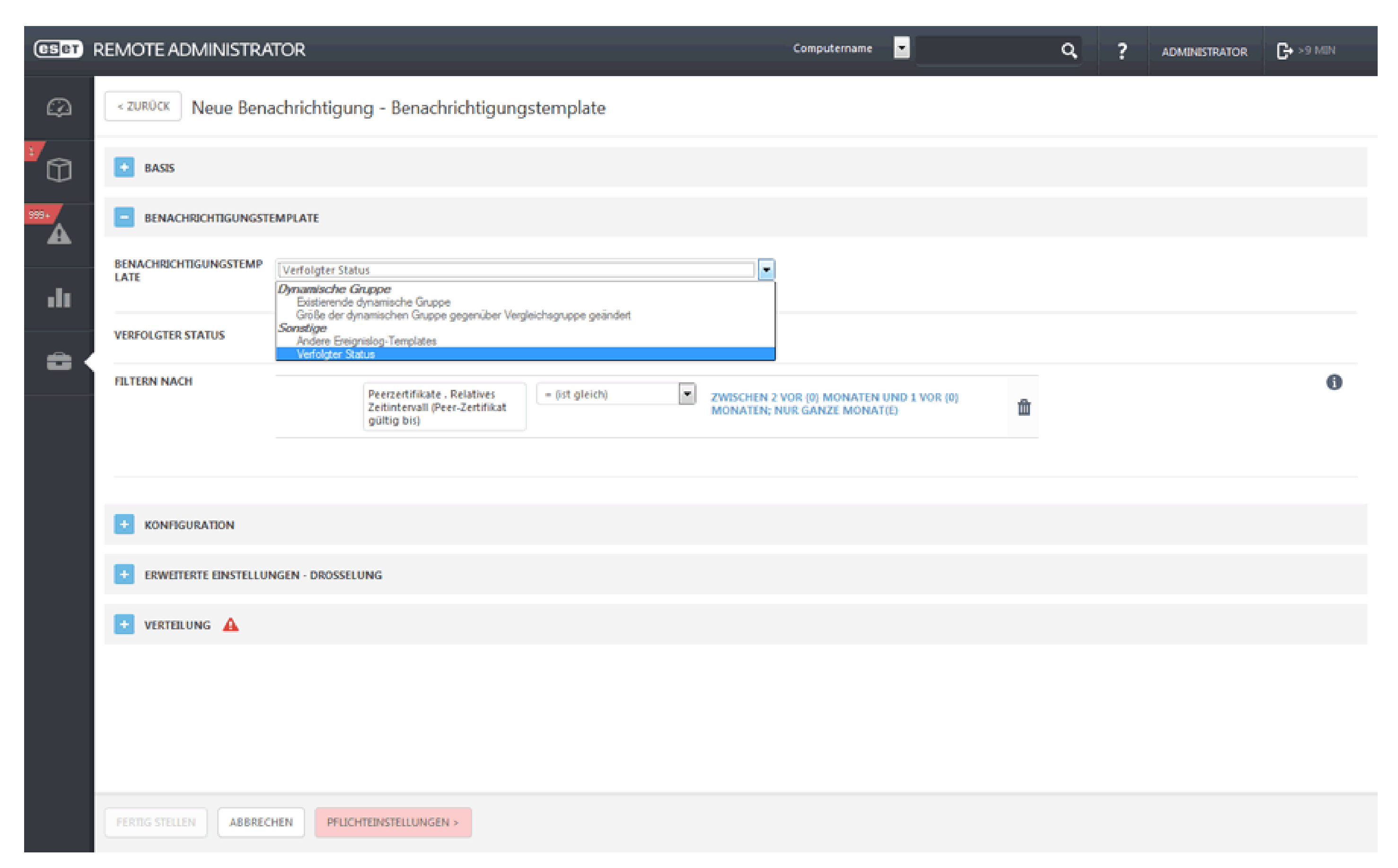
6.1.5.1 Assistent für Benachrichtigungen

Basis

Enthält **Name** und **Beschreibung** der Benachrichtigung. Diese Angaben sind hilfreich zum Filtern mehrerer Benachrichtigungen. Der Filter befindet sich oben auf der Seite **Benachrichtigung**.



Benachrichtigungstemplate



Existierende dynamische Gruppe - Für die Generierung von Benachrichtigungen wird eine existierende dynamische Gruppe verwendet. Wählen Sie eine dynamische Gruppe aus der Liste aus und klicken Sie auf **OK**.
Größe der dynamischen Gruppe gemäß Schwellenwert geändert - Wenn die Anzahl der Clients in einer beobachteten dynamischen Gruppe sich im Vergleich zu einer (statischen oder dynamischen) Vergleichsgruppe ändert, wird die Benachrichtigung ausgelöst.**Andere Ereignislog-Templates -** Diese Option wird für Benachrichtigungen verwendet, die nicht mit einer dynamischen Gruppe verknüpft sind, sondern auf Systemereignissen basieren, die aus dem Ereignislog gefiltert werden. Wählen Sie einen **Logtyp** aus, auf dem die Benachrichtigung basieren soll, und treffen Sie eine Auswahl für **Logischer Operator für Filter**.

Verfolgter Status - Mit dieser Option werden Benachrichtigungen auf Grundlage benutzerdefinierter Filter bei einer Änderung des Objektstatus ausgelöst.

Konfiguration

Benachrichtigung bei jeder Änderung des Inhalts der dynamischen Gruppe - Aktivieren Sie diese Option, um eine Benachrichtigung zu erhalten, wenn Mitglieder einer dynamischen Gruppe hinzugefügt, entfernt oder geändert werden.
Benachrichtigungs-Zeitintervall - Legen Sie das Zeitintervall (in Minuten, Stunden oder Tagen) für den Vergleich mit dem neuen Status fest. Beispiel: Vor 7 Tagen waren auf 10 Clients veraltete Sicherheitslösungen vorhanden und der **Schwellenwert** (siehe unten) wurde auf 20 festgelegt. Wenn die Anzahl der Clients mit veralteten Sicherheitslösungen 30 erreicht, erhalten Sie eine Benachrichtigung.

Schwellenwert - Legen Sie einen Schwellenwert fest, der das Senden einer Benachrichtigung auslöst. Sie können entweder eine Anzahl Clients oder einen Prozentsatz der Clients (Mitglieder einer dynamischen Gruppe) festlegen.
Generierte Nachricht - Dies ist die vordefinierte Nachricht, die in der Benachrichtigung angezeigt wird. Sie enthält konfigurierte Einstellungen im Textformat.
Nachricht - Neben der vordefinierten Nachricht können Sie eine benutzerdefinierte Nachricht hinzufügen. Diese wird am Ende der oben beschriebenen, vordefinierten Nachricht angezeigt. Die benutzerdefinierte Nachricht ist optional, ihre Eingabe wird jedoch zur einfacheren Filterung der Benachrichtigungen empfohlen.

HINWEIS: Die Konfigurationsoptionen können je nach Benachrichtigungstemplate abweichen.

Erweiterte Einstellungen - Drosselung

Zeitbasierte Kriterien

- Geben Sie die **Anzahl zu aggregierender Ticks** an. Dies legt fest, wie viele Triggertreffer benötigt werden, um den Trigger zu aktivieren. Weitere Informationen finden Sie im Kapitel Drosselung.

Statistische Kriterien

- **Anwendung statistischer Kriterien** - Diese Option legt fest, mit welcher Methode die statistischen Kriterien bewertet werden. Es müssen entweder alle Kriterien (**AND**) oder mindestens ein Kriterium (**OR**) erfüllt werden.
- **Ausgelöst je Anzahl Vorkommnisse** - Nur jeden **X.** Treffer zulassen. Wenn Sie beispielsweise „10“ eingeben, wird nur jeder 10. Treffer gezählt.
- **Anzahl Vorkommnisse über ein Zeitintervall** - Nur Treffer im definierten Zeitintervall zulassen. Diese Option legt die Frequenz fest. Sie können beispielsweise festlegen, dass der Task ausgeführt wird, wenn das Ereignis innerhalb von einer Stunde 10 Mal auftritt. Zeitraum - Definieren Sie hier den Zeitraum für die oben beschriebene Option.
- **Anzahl Ereignisse mit Symbol** - Treffer zulassen, wenn **X** Ereignisse mit dem angegebenen Symbol eingetreten sind. Wenn Sie beispielsweise „10“ eingeben, wird ein Treffer je 10 Installationen einer bestimmten Software gezählt. Gilt für Anzahl von Ereignissen - Geben Sie an, nach wie vielen aufeinanderfolgenden Ereignissen nach dem letzten Treffer ein weiterer Treffer gezählt werden soll. Wenn Sie beispielsweise „10“ eingeben, wird 10 Ereignisse nach dem letzten Treffer ein neuer Treffer gezählt.
- **Gilt für Anzahl von Ereignissen** - Sie können festlegen, ob zur Anwendung des Triggers die in Serie empfangenen Treffer (**Empfangen in Serie**; die Triggerausführung wird nicht berücksichtigt) oder die Treffer seit der letzten Triggerausführung (**Empfangen seit letzter Triggerausführung**, d. h. beim Ausführen des Triggers wird der Zähler auf 0 zurückgesetzt) berücksichtigt werden.

Verteilung

Betreff - Betreff der Nachricht, die die Benachrichtigung enthält. Die Angabe ist optional, wird jedoch zur Vereinfachung der Filterung und zur Verwendung von Sortierregeln für die Benachrichtigungen empfohlen.

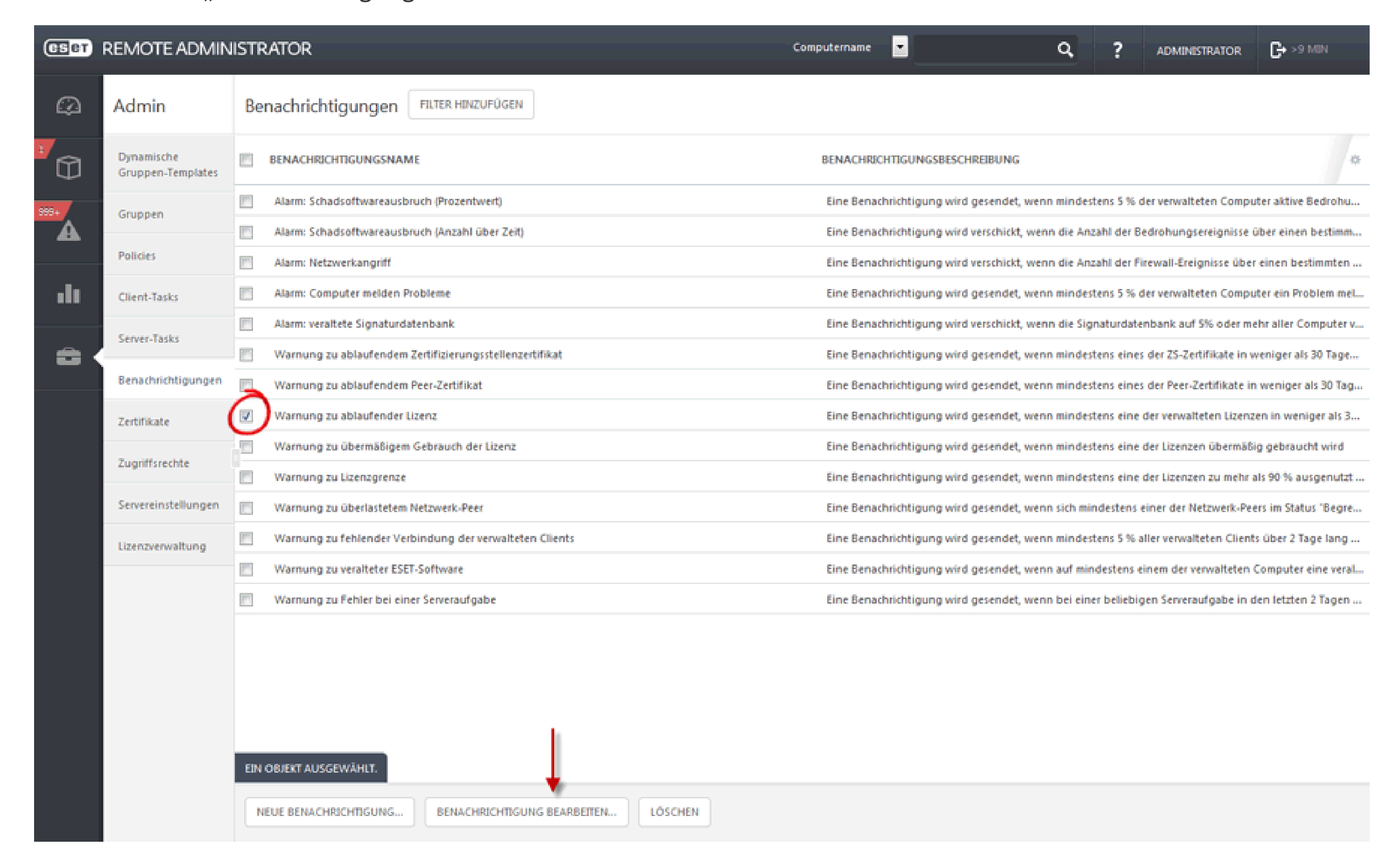
Verteilung

- **SNMP-Trap senden** - Sendet ein SNMP-Trap. Der SNMP-Trap benachrichtigt den Server mit einer nicht angeforderten SNMP-Nachricht. Weitere Informationen finden Sie unter Konfigurieren eines SNMP-Trap-Dienstes.
- **E-mail senden** - Sendet eine E-Mail-Nachricht auf Grundlage der E-Mail-Einstellungen.

E-Mail-Adressen - Geben Sie die E-Mail-Adressen der Empfänger der Benachrichtigungen ein. Trennen Sie mehrere Adressen durch ein Komma („**,**“).

6.1.5.2 Verwalten von Benachrichtigungen

Benachrichtigungen werden auf der Registerkarte „Admin“ verwaltet. Wählen Sie eine Benachrichtigung aus und klicken Sie auf „Benachrichtigung bearbeiten“.



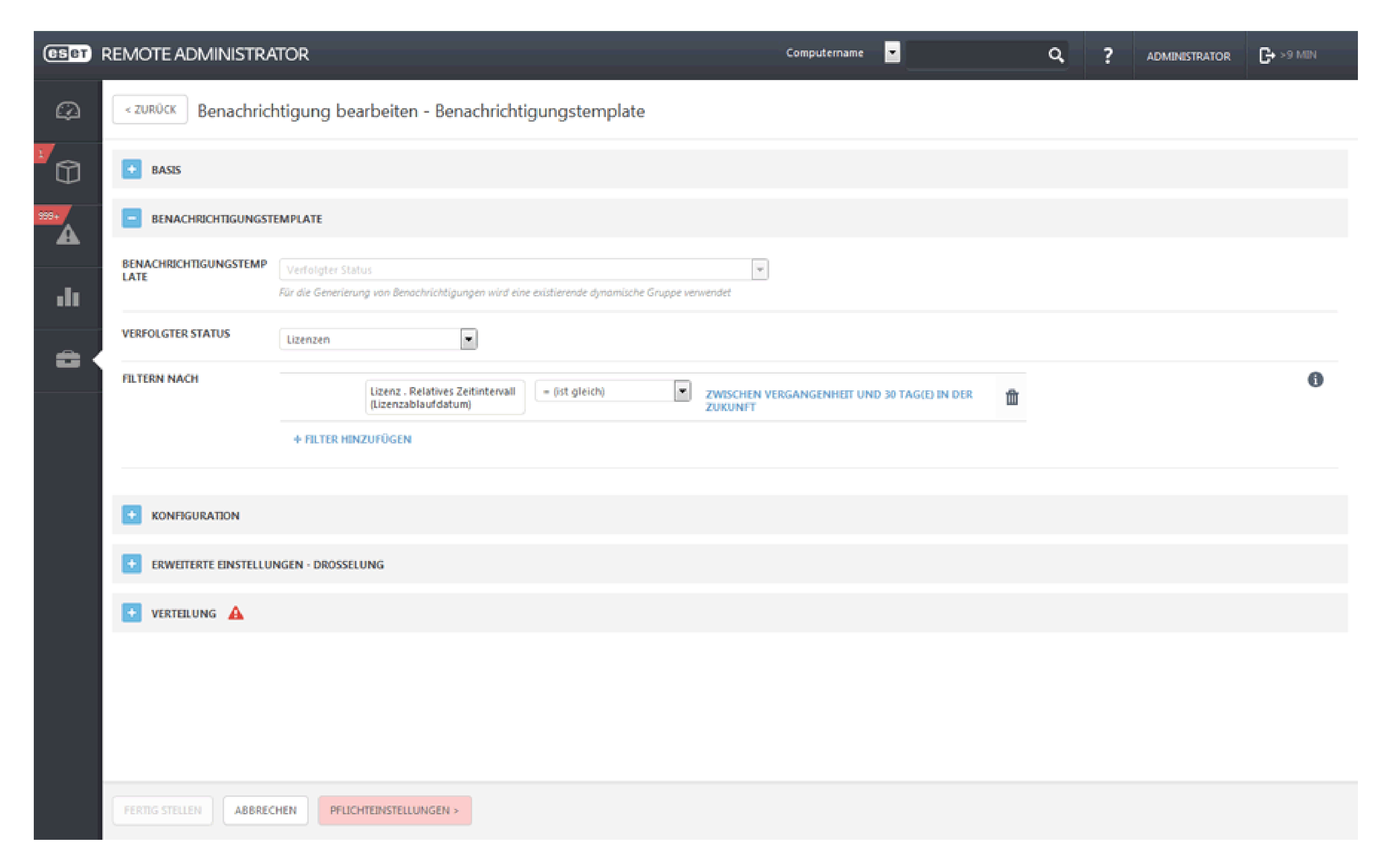
Basis

Hier können Sie die Angaben unter **Benachrichtigungsname** und **Beschreibung** ändern. Diese Angaben sind wichtig für das Anwenden von Filtern, wenn mehrere Benachrichtigungen verfügbar sind.

Benachrichtigungstemplate

Existierende dynamische Gruppe - Für die Generierung von Benachrichtigungen wird eine existierende dynamische Gruppe verwendet. Wählen Sie eine dynamische Gruppe aus der Liste aus und klicken Sie auf **OK**.
Größe der dynamischen Gruppe gegenüber Vergleichsgruppe geändert - Wenn die Anzahl der Clients in einer beobachteten dynamischen Gruppe sich gegenüber einer (statischen oder dynamischen) Vergleichsgruppe ändert, wird die Benachrichtigung ausgelöst.
Andere Ereignislog-Templates
Diese Option wird für Benachrichtigungen verwendet, die nicht mit einer dynamischen Gruppe verknüpft sind, sondern auf Systemereignissen basieren, die aus dem Ereignislog gefiltert wurden. Wählen Sie einen **Logtyp** aus, auf dem die Benachrichtigung basieren soll, und treffen Sie eine Auswahl für **Logischer Operator für Filter**.
Verfolgter Status - Mit dieser Option werden Benachrichtigungen auf Grundlage benutzerdefinierter Filter bei einer Änderung des Objektstatus ausgelöst.

HINWEIS: Sie können den verfolgten Status ändern oder die Funktionen **+ Filter hinzufügen** oder **Logischer Operator für Filter** verwenden.



Konfiguration

Benachrichtigen, wenn sich der Inhalt der dynamischen Gruppe ändert - Aktivieren Sie diese Option, um eine Benachrichtigung zu erhalten, wenn Mitglieder einer dynamischen Gruppe hinzugefügt, entfernt oder geändert werden.
Benachrichtigungs-Zeitintervall - Legen Sie das Zeitintervall (in Minuten, Stunden oder Tagen) für den Vergleich mit dem neuen Status fest. Beispiel: Vor 7 Tagen waren auf 10 Clients veraltete Sicherheitslösungen vorhanden und der **Schwellenwert** (siehe unten) wurde auf 20 festgelegt. Wenn die Anzahl der Clients mit veralteten Sicherheitslösungen 30 erreicht, erhalten Sie eine Benachrichtigung.
Schwellenwert - Legen Sie einen Schwellenwert fest, der das Senden einer Benachrichtigung auslöst. Sie können entweder eine Anzahl Clients oder einen Prozentsatz der Clients (Mitglieder der dynamischen Gruppe) festlegen.
Generierte Nachricht - Dies ist die vordefinierte Nachricht, die in der Benachrichtigung angezeigt wird. Sie enthält konfigurierte Einstellungen im Textformat.
Nachricht - Neben der vordefinierten Nachricht können Sie eine benutzerdefinierte Nachricht hinzufügen. Diese wird am Ende der oben beschriebenen, vordefinierten Nachricht angezeigt. Die benutzerdefinierte Nachricht ist optional, ihre Eingabe wird jedoch zur einfacheren Filterung der Benachrichtigungen und zur besseren Übersichtlichkeit empfohlen.

HINWEIS: Die verfügbaren Optionen hängen vom ausgewählten Benachrichtigungstemplate ab.

Erweiterte Einstellungen - Drosselung

Zeitbasierte Kriterien

- Geben Sie die **Anzahl zu aggregierender Ticks** an. Dies legt fest, wie viele Triggertreffer benötigt werden, um den Trigger zu aktivieren. Weitere Informationen finden Sie im Kapitel Drosselung.

Statistische Kriterien

- **Anwendung statistischer Kriterien** - Diese Option legt fest, mit welcher Methode die statistischen Kriterien bewertet werden. Es müssen entweder alle Kriterien (**AND**) oder mindestens ein Kriterium (**OR**) erfüllt werden.
- **Ausgelöst je Anzahl Vorkommnisse** - Nur jeden **X.** Treffer zulassen. Wenn Sie beispielsweise „10“ eingeben, wird nur jeder 10. Treffer gezählt.
- **Anzahl Vorkommnisse über ein Zeitintervall** - Nur Treffer im definierten Zeitintervall zulassen. Diese Option legt die Frequenz fest. Sie können beispielsweise festlegen, dass der Task ausgeführt wird, wenn das Ereignis innerhalb von einer Stunde 10 Mal auftritt. Zeitraum - Definieren Sie hier den Zeitraum für die oben beschriebene Option.
- **Anzahl Ereignisse mit Symbol** - Treffer zulassen, wenn **X** Ereignisse mit dem angegebenen Symbol eingetreten sind. Wenn Sie beispielsweise „10“ eingeben, wird ein Treffer je 10 Installationen einer bestimmten Software gezählt. **Gilt für Anzahl von Ereignissen** - Geben Sie an, nach wie vielen aufeinanderfolgenden Ereignissen nach dem letzten Treffer ein weiterer Treffer gezählt werden soll. Wenn Sie beispielsweise „10“ eingeben, wird 10 Ereignisse nach dem letzten Treffer ein neuer Treffer gezählt.
- **Gilt für Anzahl von Ereignissen** - Sie können festlegen, ob zur Anwendung des Triggers die in Serie empfangenen Treffer (**Empfangen in Serie**; die Triggerausführung wird nicht berücksichtigt) oder die Treffer seit der letzten Triggerausführung (**Empfangen seit letzter Triggerausführung**, d. h. beim Ausführen des Triggers wird der Zähler auf 0 zurückgesetzt) berücksichtigt werden.

Verteilung

Betreff - Betreff der Nachricht, die die Benachrichtigung enthält. Die Angabe ist optional, wird jedoch zur Vereinfachung der Filterung und zur Verwendung von Sortierregeln für die Nachrichten empfohlen.

Verteilung

- **SNMP-Trap senden** - Sendet ein SNMP-Trap. Der SNMP-Trap benachrichtigt den Server mit einer nicht angeforderten SNMP-Nachricht. Weitere Informationen finden Sie unter Konfigurieren eines SNMP-Trap-Dienstes.
- **E-mail senden** - Sendet eine E-Mail-Nachricht auf Grundlage der E-Mail-Einstellungen.

E-Mail-Adressen - Geben Sie die E-Mail-Adressen der Empfänger der Benachrichtigungen ein. Trennen Sie mehrere Adressen durch ein Komma („**,**“).

6.1.5.3 Konfigurieren eines SNMP-Trap-Dienstes

Zum erfolgreichen Empfangen von SNMP-Nachrichten muss der SNMP-Trap-Dienst konfiguriert werden.

Konfigurationsschritte für verschiedene Betriebssysteme

- Windows
- Linux

WINDOWS

Voraussetzungen

- Der **Simple Network Management Protocol**-Dienst muss auf dem Computer, auf dem der ERA-Server installiert wird, und auf dem Computer, auf dem die SNMP-Trap-Software installiert werden soll, installiert sein.
- Beide Computer müssen sich im gleichen Subnetz befinden.
- Der SNMP-Dienst wird auf dem ERA-Server-Computer konfiguriert.

Konfiguration des SNMP-Dienstes (ERA-Server)

- Drücken Sie die Windows-Tasten und den Buchstaben „R", um das Dialogfeld „Ausführen" zu öffnen. Geben Sie *Services.msc* in das Feld **Öffnen** ein und drücken Sie die Eingabetaste. Suchen Sie den SNMP-Dienst.
- Öffnen Sie die Registerkarte **Traps**, geben Sie **„public"** in das Feld **Communityname** ein und klicken Sie auf **Zur Liste hinzufügen**.
- Klicken Sie auf **Hinzufügen** und geben Sie in das entsprechende Feld den **Hostnamen**, die IP-Adresse oder die **IPX-Adresse** des Computers ein, auf dem die SNMP-Trap-Software installiert ist. Klicken Sie dann auf **Hinzufügen**.
- Wechseln Sie zur Registerkarte **Sicherheit**. Klicken Sie auf **Hinzufügen**, um das Fenster **SNMP-Dienstkonfiguration** zu öffnen. Geben Sie **public** in das Feld **Communityname** ein und klicken Sie auf **Hinzufügen**. Die Rechte werden auf **schreibgeschützt** festgelegt. Dies ist in Ordnung.
- Vergewissern Sie sich, dass **SNMP-Pakete von jedem Host annehmen** ausgewählt ist und klicken Sie zur Bestätigung auf **OK**. Der SNMP-Dienst ist nicht konfiguriert.

Konfiguration der SNMP-Trap-Software (Client)

- Der SNMP-Dienst ist installiert und muss nicht konfiguriert werden.
- Installieren Sie **AdRem SNMP Manager** oder **AdRem NetCrunch**.
- **AdRem SNMP Manager**: Starten Sie die Anwendung und wählen Sie **Neue SNMP-Knotenliste erstellen** aus. Klicken Sie zur Bestätigung auf **Ja**.
- Überprüfen Sie die Netzwerkadresse des Subnetzes (in diesem Fenster angezeigt). Klicken Sie auf **OK**, um das Netzwerk zu durchsuchen.
- Warten Sie, bis die Suche abgeschlossen ist. Die Suchergebnisse werden im Fenster **Ergebnisse der Ermittlung** angezeigt. Die IP-Adresse des ERA-Servers sollte in dieser Liste angezeigt werden.
- Wählen Sie die IP-Adresse des Servers aus und klicken Sie auf **OK**. Die Serveradresse wird im Bereich **Knoten** angezeigt.
- Klicken Sie auf **Trap-Empfänger gestoppt** und wählen Sie **Starten** aus. **Trap-Empfänger gestartet** wird angezeigt. Sie können nun SNMP-Nachrichten vom ERA-Server empfangen.

LINUX

1. Installieren Sie das snmpd-Paket, indem Sie einen der folgenden Befehle ausführen:
   `apt-get install snmpd snmp` (Debian-, Ubuntu-Verteilungen)
   `yum install net-snmp` (Red-Hat-, Fedora-Verteilungen)

2. Öffnen Sie die Datei */etc/default/snmpd* und bearbeiten Sie die Attribute:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```
Das Symbol # deaktiviert die Zeile vollständig.

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/snmpd.conf'
```
Fügen Sie diese Zeile zur Datei hinzu.

```
TRAPDRUN=yes
```
Ändern Sie das Attribut *trapdrun* zu *yes*.

3. Erstellen Sie eine Sicherung der ursprünglichen *snmpd.conf*-Datei. Die Datei wird später bearbeitet.

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. Erstellen Sie eine neue *snmpd.conf*-Datei und fügen Sie folgende Zeilen hinzu:

```
rocommunity public
syslocation "Testing ERA6"
syscontact admin@ERA6.com
```

5. Öffnen Sie die Datei */etc/snmp/snmptrapd.conf* und fügen Sie am Ende der Datei die folgende Zeile hinzu:

```
authCommunity log,execute,net public
```

6. Geben Sie den folgenden Befehl ein, um die SNMP-Dienste und das Protokollieren eingehender Traps zu starten:

```
/etc/init.d/snmpd restart
```
oder
```
service snmpd restart
```

7. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Trap funktioniert und Nachrichten abfängt:

```
tail -f /var/log/syslog | grep -i TRAP
```

6.1.6 Zertifikate

Ein Zertifikat authentifiziert die bei der Kommunikation zwischen dem ERA-Server und dem Agenten ausgetauschten Daten, weil der ERA-Server ebenfalls über einen Agenten kommuniziert.

- Erstellen eines neuen Zertifikats mit der ERA-Zertifizierungsstelle
- Erstellen eines neuen Zertifikats mit einer benutzerdefinierten Zertifizierungsstelle
- Erstellen einer neuen Zertifizierungsstelle

6.1.6.1 Peerzertifikate

Ein Zertifikat authentifiziert die Daten der Kommunikation zwischen dem ERA-Server und dem Agenten, weil der ERA-Server ebenfalls über einen Agenten kommuniziert.

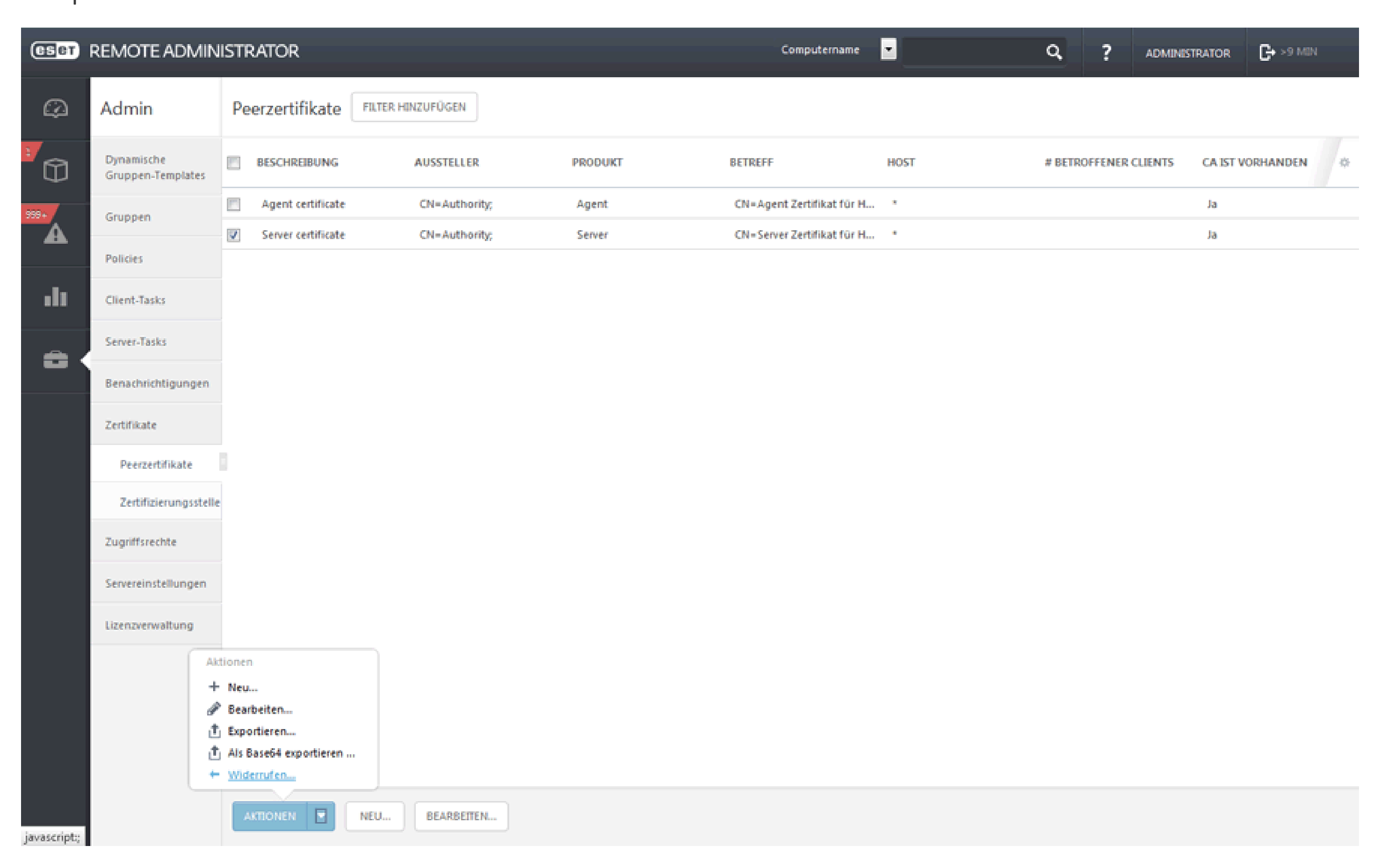
+ **Neu ...** - Diese Option ermöglicht die Erstellung eines neuen Zertifikats mit der ERA-Zertifizierungsstelle oder die Erstellung eines neuen Zertifikats mit einer benutzerdefinierten Zertifizierungsstelle. Diese Zertifikate werden für den Agenten, den Proxy und den Server verwendet.

Bearbeiten ... - Wählen Sie diese Option aus, um ein in der Liste vorhandenes Zertifikat zu bearbeiten. Es stehen die gleichen Optionen wie beim Erstellen eines neuen Zertifikats zur Verfügung.

Exportieren ... - Mit dieser Option können Sie das Zertifikat als Datei exportieren. Diese Datei ist erforderlich, wenn Sie den Agenten lokal auf einem Computer installieren oder wenn Sie den Connector für Mobilgeräte installieren.

Als Base64 exportieren ... - Mit dieser Option können Sie das Zertifikat als TXT-Datei exportieren.

Widerrufen ... - Wenn Sie das Zertifikat nicht mehr verwenden möchten, wählen Sie „Widerrufen" aus. Mit dieser Option wird das Zertifikat ungültig gemacht. Ungültige Zertifikate werden von ESET Remote Administrator nicht akzeptiert.

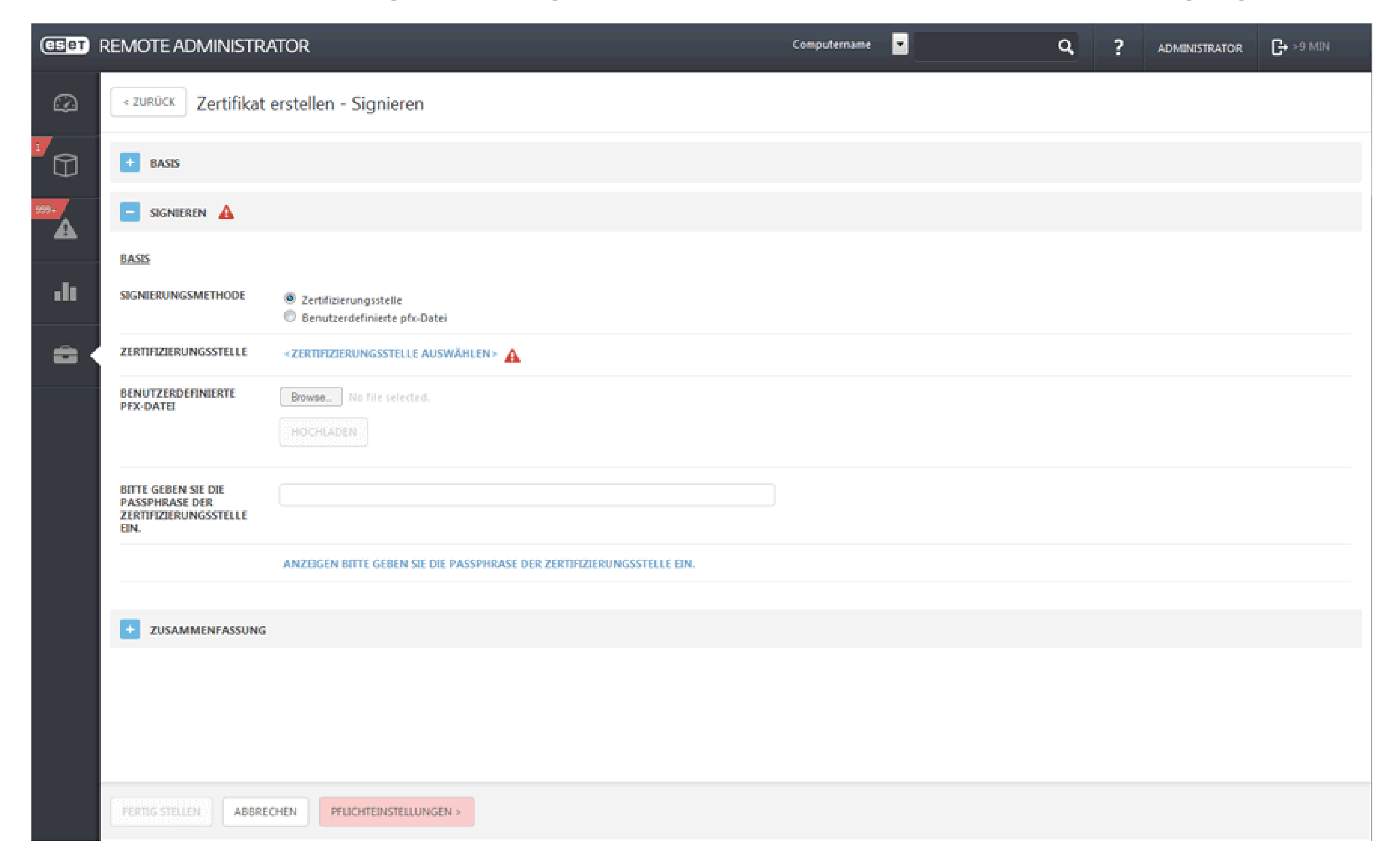


6.1.6.1.1 Erstellen eines neuen Zertifikats mit der ERA-Zertifizierungsstelle

Um eine neue Behörde in der **ERA Web-Konsole** zu erstellen, navigieren Sie zu **Admin** > **Zertifikate** und klicken Sie auf **Aktionen** > **Neu**.

Basis

- Geben Sie eine **Beschreibung** für das Zertifikat ein und wählen Sie den **Agenten** als **Produkt** aus.
- Geben Sie Verbindungsinformationen für den ERA-Server im Feld **Host** ein. Sie können einen Hostnamen, eine IP-Adresse oder einen Teil des Namens mit Platzhalter („*“) eingeben. Mehrere Einträge werden durch Leerzeichen ( ), Kommas (,) oder Strichpunkte (;) getrennt.
- Geben Sie im Feld **Passphrase** und im Bestätigungsfeld ein Passwort ein. Dieses Passwort wird während der Installation des Agenten verwendet.
- Geben Sie einen Wert in das Feld **Allgemeiner Name** ein. Der Wert sollte die Zeichenfolge „Agent“, „Proxy“ oder „Server“ enthalten, je nachdem, welches **Produkt** ausgewählt wurde.
- Wenn Sie möchten, können Sie beschreibende Informationen zum Zertifikat eingeben.
- Geben Sie in die Felder **Gültig ab** und **Gültig bis** Werte ein, um sicherzustellen, dass das Zertifikat gültig ist.



Signieren

- Die Signierungsmethode sollte auf **Zertifizierungsstelle** eingestellt sein.
- Wählen Sie die **ERA-Zertifizierungsstelle** aus, die bei der ursprünglichen Installation erstellt wurde.
- Überspringen Sie die Option für eine benutzerdefinierte `pfx` -Datei. Diese Option gilt nur für selbstsignierte `pfx` -Zertifikatsbehörden.
- Geben Sie das Passwort für das Zertifikat ein. Das Passwort ist die **Passphrase der Zertifizierungsstelle**, die während der Serverinstallation erstellt wurde.

Zusammenfassung

- Überprüfen Sie die eingegebenen Zertifikatinformationen und klicken Sie auf **Fertig stellen**. Nach der erfolgreichen Erstellung ist das Zertifikat bei der Installation des Agenten in der Liste **Zertifikate** verfügbar.

6.1.6.1.2 Erstellen eines neuen Zertifikats mit einer benutzerdefinierten Zertifizierungsstelle

Um eine neue Behörde in der **ERA Web-Konsole** zu erstellen, navigieren Sie zu **Admin** > **Zertifikate** und klicken Sie auf **Aktionen** > **Neu**.

Basis

- Geben Sie eine **Beschreibung** für das Zertifikat ein und wählen Sie den **Agenten** als **Produkt** aus.
- Geben Sie Verbindungsinformationen für den ERA-Server im Feld **Host** ein. Sie können einen Hostnamen, eine IP-Adresse oder einen Teil des Namens mit Platzhalter („*“) eingeben. Mehrere Einträge werden durch Leerzeichen ( ), Kommas (,) oder Strichpunkte (;) getrennt.
- Geben Sie im Feld **Passphrase** und im Bestätigungsfeld ein Passwort ein. Dieses Passwort wird während der Installation des Agenten verwendet.
- Geben Sie einen Wert in das Feld **Allgemeiner Name** ein. Der Wert sollte die Zeichenfolge „Agent“, „Proxy“ oder „Server“ enthalten, je nachdem, welches **Produkt** ausgewählt wurde.
- Wenn Sie möchten, können Sie beschreibende Informationen zum Zertifikat eingeben.
- Geben Sie in die Felder **Gültig ab** und **Gültig bis** Werte ein, um sicherzustellen, dass das Zertifikat gültig ist.

Signieren

- Die Signierungsmethode sollte auf **Benutzerdefinierte pfx-Datei** festgelegt werden.
- Klicken Sie auf **Durchsuchen**, um eine benutzerdefiniertepfx-Datei auszuwählen. Navigieren Sie zur benutzerdefiniertenpfx-Datei und klicken Sie auf **OK**. Klicken Sie auf **Hochladen**, um das Zertifikat auf den Server hochzuladen.
- Geben Sie das Passwort für das Zertifikat ein. Das Passwort ist die **Passphrase der Zertifizierungsstelle**, die während der Serverinstallation erstellt wurde.

Zusammenfassung

- Überprüfen Sie die eingegebenen Zertifikatinformationen und klicken Sie auf **Fertig stellen**. Nach der erfolgreichen Erstellung des Zertifikats kann es für die Installation des Agenten verwendet werden.

6.1.6.2 Zertifikatsbehörden

Im Abschnitt **Zertifikatsbehörden** werden die Zertifikatsbehörden aufgeführt und verwaltet. Wenn mehrere Zertifikatsbehörden vorhanden sind, kann es hilfreich sein, die Anzeige über einen Filter zu sortieren.

Klicken Sie oben auf der Seite auf **Filter hinzufügen** und wählen Sie die gewünschten Filterkriterien aus (Beschreibung, Betreff, gültig von /bis usw.). Sie können ein Kriterium je Filter festlegen. Wenn Sie eines der Kriterien auswählen und auf „OK“ klicken, wird neben der Schaltfläche „Filter hinzufügen“ ein Textfeld geöffnet. In das Textfeld können Sie benutzerdefinierte Informationen eingeben, beispielsweise ein **Datum** oder eine **Beschreibung**. Klicken Sie auf „Filter hinzufügen“, um einen zusätzlichen Filter hinzuzufügen. Sie können beliebig viele Filter erstellen.

6.1.6.2.1 Erstellen einer neuen Zertifizierungsstelle

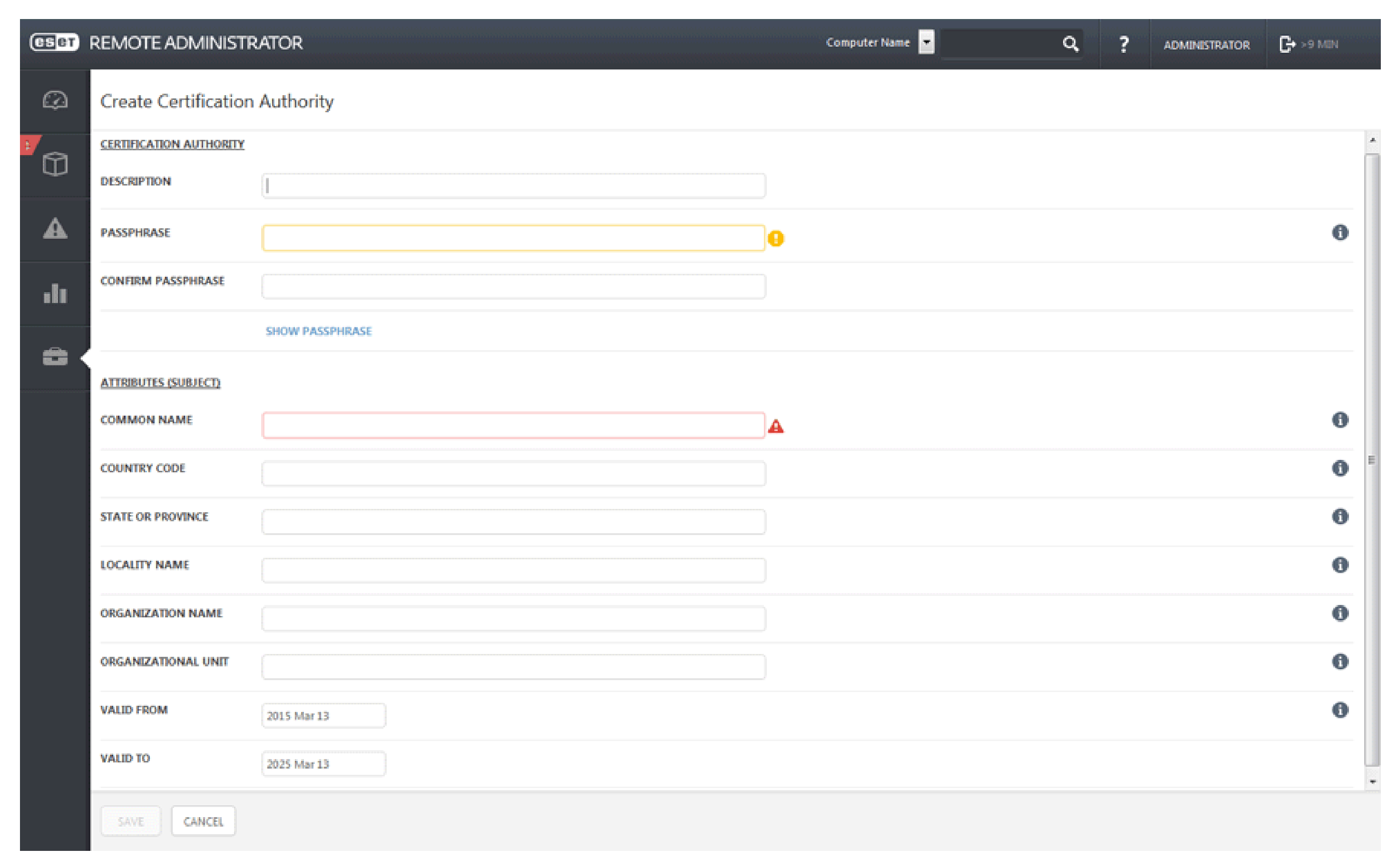
Um eine neue Zertifizierungsstelle zu erstellen, navigieren Sie zu **Admin** > **Zertifikate** > **Zertifizierungsstelle** und klicken Sie auf **Aktion** > **+ Neu...**, oder **Neu** unten auf der Seite.

Zertifizierungsstelle

Geben Sie eine **Beschreibung** der Zertifizierungsstelle ein und wählen Sie eine **Passphrase** aus. Die **Passphrase** muss mindestens 12 Zeichen lang sein.

Attribute (Thema)

1. Geben Sie unter **Allgemeiner Namen** einen Namen für die Zertifizierungsstelle ein. Wählen Sie einen eindeutigen Namen aus, um mehrere Zertifikatsbehörden unterscheiden zu können.
   Optional können Sie beschreibende Informationen zur Zertifizierungsstelle eingeben.
2. Geben Sie in die Felder **Gültig ab** und **Gültig bis** Werte ein, um sicherzustellen, dass das Zertifikat gültig ist.
3. Klicken Sie auf **Speichern**, um die neue Zertifizierungsstelle zu speichern. Sie wird nun in der Liste der Zertifikatsbehörden unter **Admin** > **Zertifikate** > **Zertifizierungsstelle** aufgeführt und kann verwendet werden.



Um die Zertifizierungsstelle zu verwalten, aktivieren Sie das Kontrollkästchen neben der Zertifizierungsstelle in der Liste und verwenden Sie das Kontextmenü (klicken Sie mit der rechten Maustaste auf die Zertifizierungsstelle) oder unten auf der Seite die Schaltfläche **Aktion**. Es stehen Optionen zum **Bearbeiten** der Zertifizierungsstelle (siehe oben genannte Schritte), zum vollständigen **Löschen** der Zertifizierungsstelle und die Option **Öffentlichen Key exportieren** zur Verfügung.

Öffentlichen Key von einer Zertifizierungsstelle exportieren

1. Wählen Sie die gewünschte Zertifizierungsstelle aus der Liste aus und aktivieren Sie das Kontrollkästchen neben der Zertifizierungsstelle.
2. Wählen Sie im Kontextmenü **Öffentlichen Key exportieren** aus. Der öffentliche Key wird als *.der*-Datei exportiert. Wählen Sie einen Namen für den öffentlichen Key aus und klicken Sie auf **Speichern**.

HINWEIS: Wenn Sie die standardmäßige ERA-Zertifizierungsstelle löschen und eine neue erstellen, funktioniert dies nicht. Sie müssen die Zertifizierungsstelle dem ERA-Servercomputer zuweisen und den Dienst „ERA-Server" neu starten.

6.1.7 Zugriffsrechte

Die Zugriffsrechte in ERA können in zwei grundlegende Kategorien eingeteilt werden:

1. Zugriff auf Funktionen
2. Zugriff auf statische Gruppen

Der Zugriff auf die Elemente der beiden Kategorien muss jedem Benutzer der ERA-Web-Konsole erteilt werden.

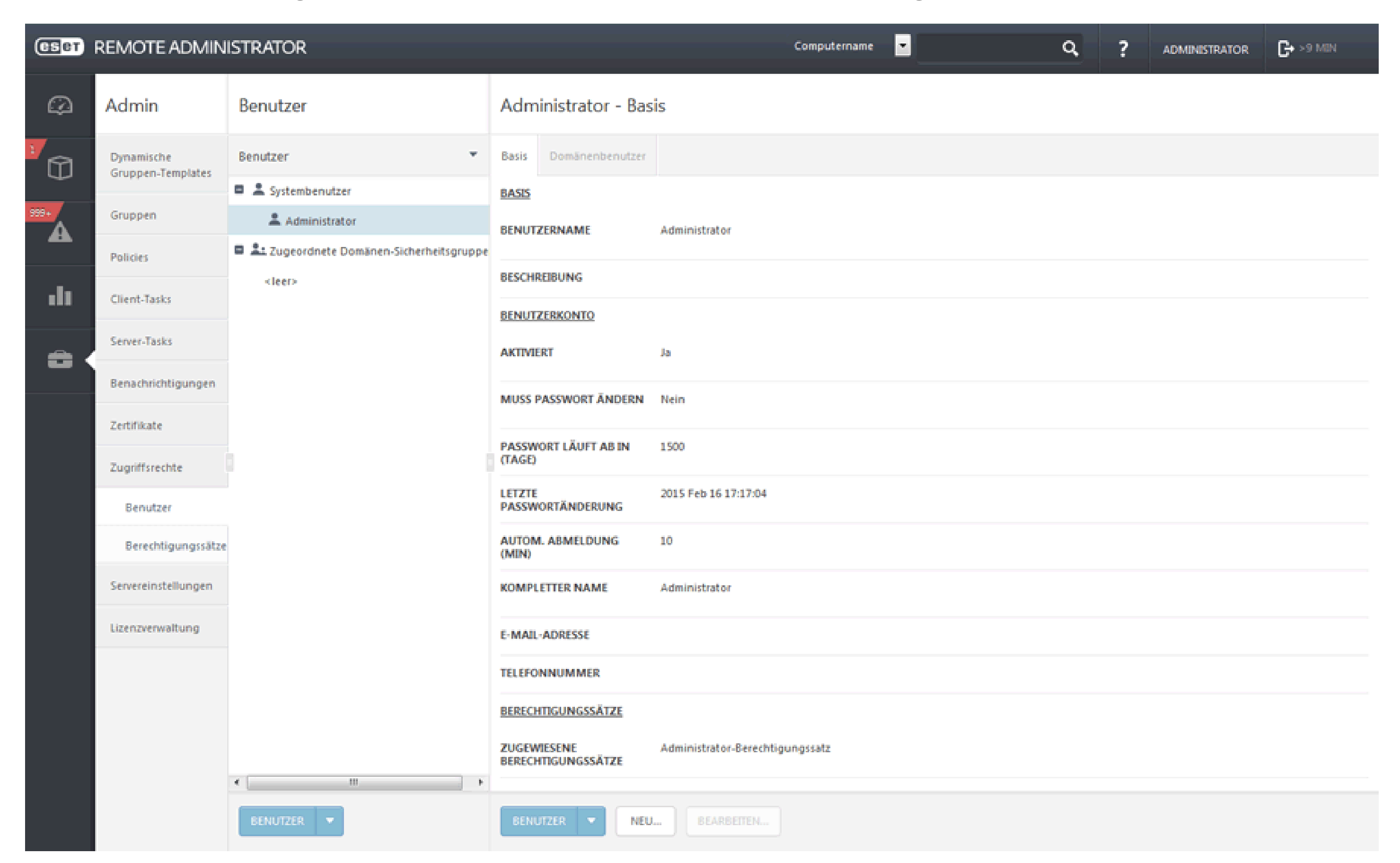
An oberster Stelle steht der Benutzer **Administrator**, der uneingeschränkten Zugriff hat. Aufgrund der sehr umfangreichen Berechtigungen kann die Verwendung dieses Kontos gefährlich sein. Es wird daher **dringend empfohlen**, zusätzliche Konten mit eingeschränkten Zugriffsrechten zu erstellen, die den erforderlichen Berechtigungen entsprechen.

Benutzer werden im Abschnitt Benutzer im Verwaltungsbereich verwaltet. Die möglichen Berechtigungen der Benutzer werden durch Berechtigungssätze dargestellt.

6.1.7.1 Benutzer

Für die ERA-Web-Konsole können Benutzer mit verschiedenen Berechtigungssätzen festgelegt werden. Der Benutzer mit den meisten Berechtigungen ist der **Administrator**. Er verfügt über volle Rechte und Berechtigungen. Zur einfacheren Arbeit mit Active Directory kann zugelassen werden, dass sich Benutzer aus Domänen-Sicherheitsgruppen bei ERA anmelden. Diese Benutzer können neben den ERA **-Systembenutzern bestehen**, die Berechtigungssätze werden dabei jedoch auf Ebene der Active Directory-Sicherheitsgruppe festgelegt, und nicht wie bei Systembenutzern für den einzelnen Benutzer.

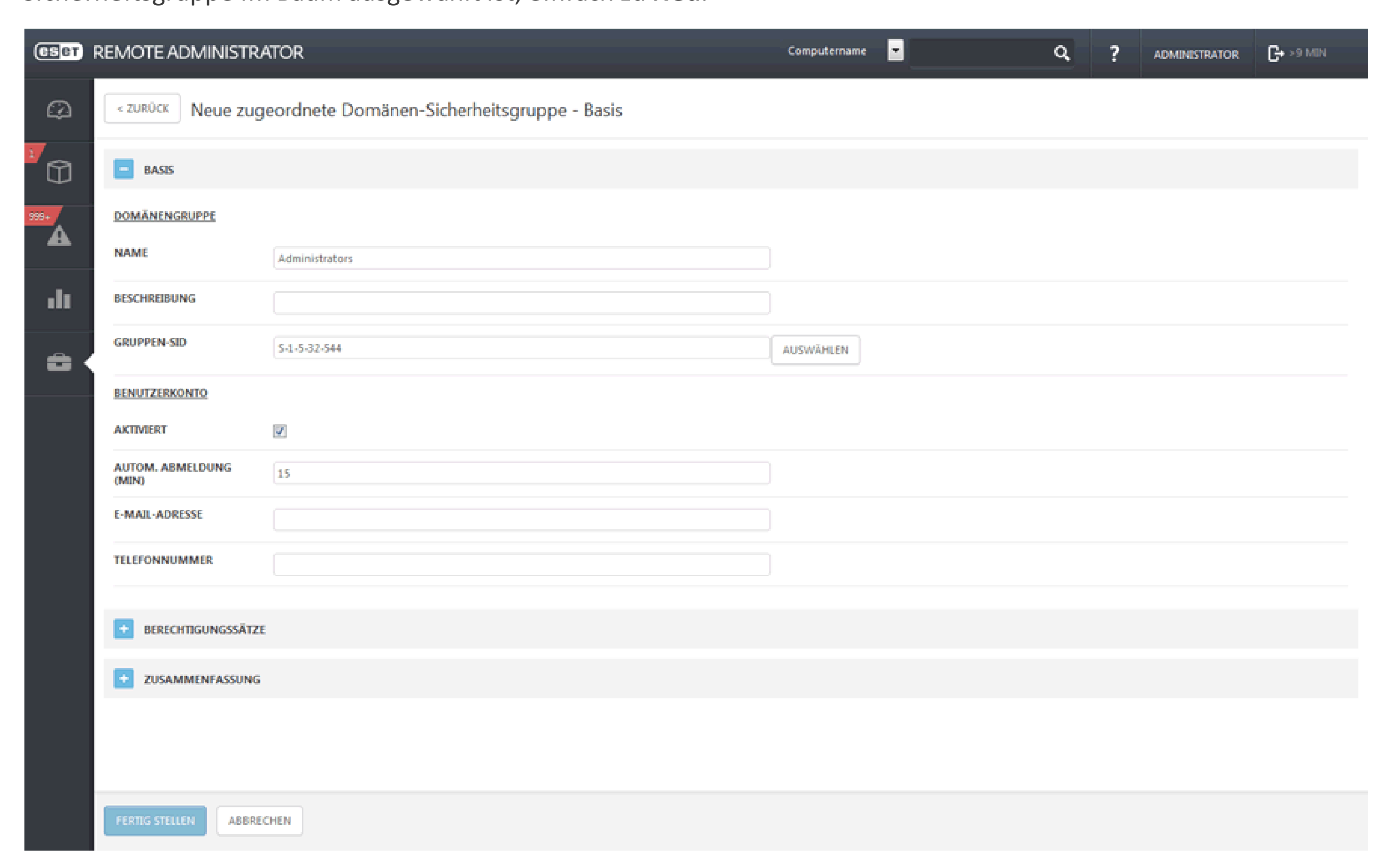
Die Benutzerverwaltung wird im Abschnitt **Admin** der ERA-Web-Konsole ausgeführt.



HINWEIS: Bei einer neuen ERA-Installation ist nur das Benutzerkonto „Administrator“ (Systembenutzer) vorhanden.

6.1.7.1.1 Assistent für zugeordnete Domänen-Sicherheitsgruppe

Um den **Assistenten für zugeordnete Domänen-Sicherheitsgruppe** zu öffnen, navigieren Sie zu **Admin** > **Zugriffsrechte** > **Zugeordnete Domänen-Sicherheitsgruppen** > **Neu** oder, wenn die zugeordnete Domänen-Sicherheitsgruppe im Baum ausgewählt ist, einfach zu **Neu**.



Basis

Domänengruppe

Geben Sie einen **Namen** für die Gruppe ein. Sie können auch eine Beschreibung der Gruppe angeben. Die Gruppe wird über eine **Gruppen-SID** (Sicherheits-ID) identifiziert. Klicken Sie auf **Auswählen**, um eine Gruppe aus der Liste auszuwählen, und dann zum Bestätigen auf **OK**.

Benutzerkonto

- Lassen Sie die Option **Aktiviert** ausgewählt, damit der Benutzer aktiv ist.
- Die Option **Autom. Abmeldung (Min)** legt fest, nach wie vielen Minuten Inaktivität der Benutzer automatisch von der ERA Web-Konsole abgemeldet wird.
- Die Angaben **E-Mail-Adresse** und **Telefonnummer** sind fakultativ und dienen der Identifizierung des Benutzers.

Berechtigungssatz

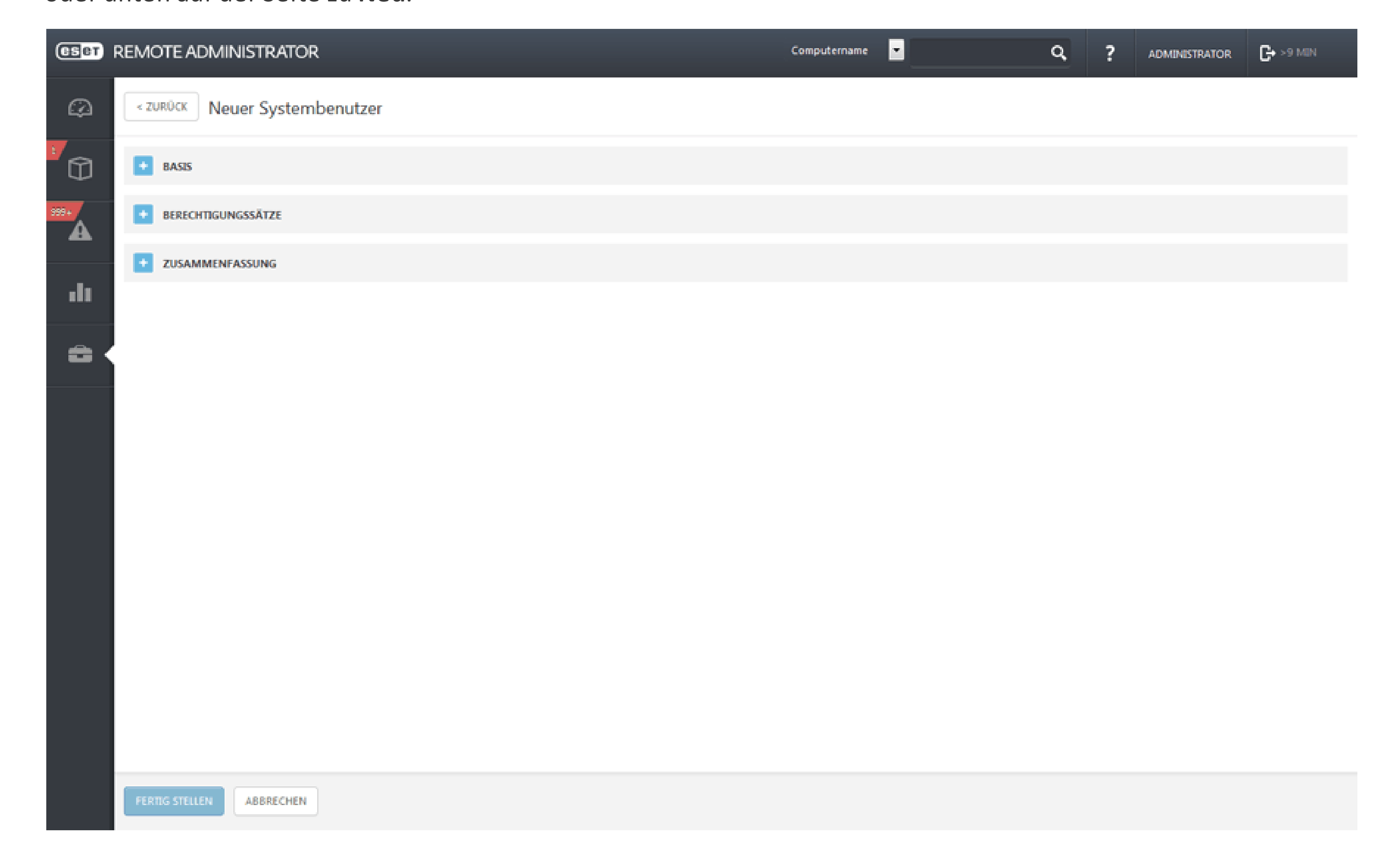
Weisen Sie dem Benutzer Berechtigungen (Rechte) zu. Sie können einen vordefinierten Berechtigungssatz verwenden: **Prüfer-Berechtigungssatz** (ähnlich Lesezugriff) und **Administrator-Berechtigungssatz** (ähnlich Vollzugriff). Alternativ können Sie einen benutzerdefinierten Berechtigungssatz erstellen.

Zusammenfassung

Überprüfen Sie die für den Benutzer konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**, um die Gruppe zu erstellen.

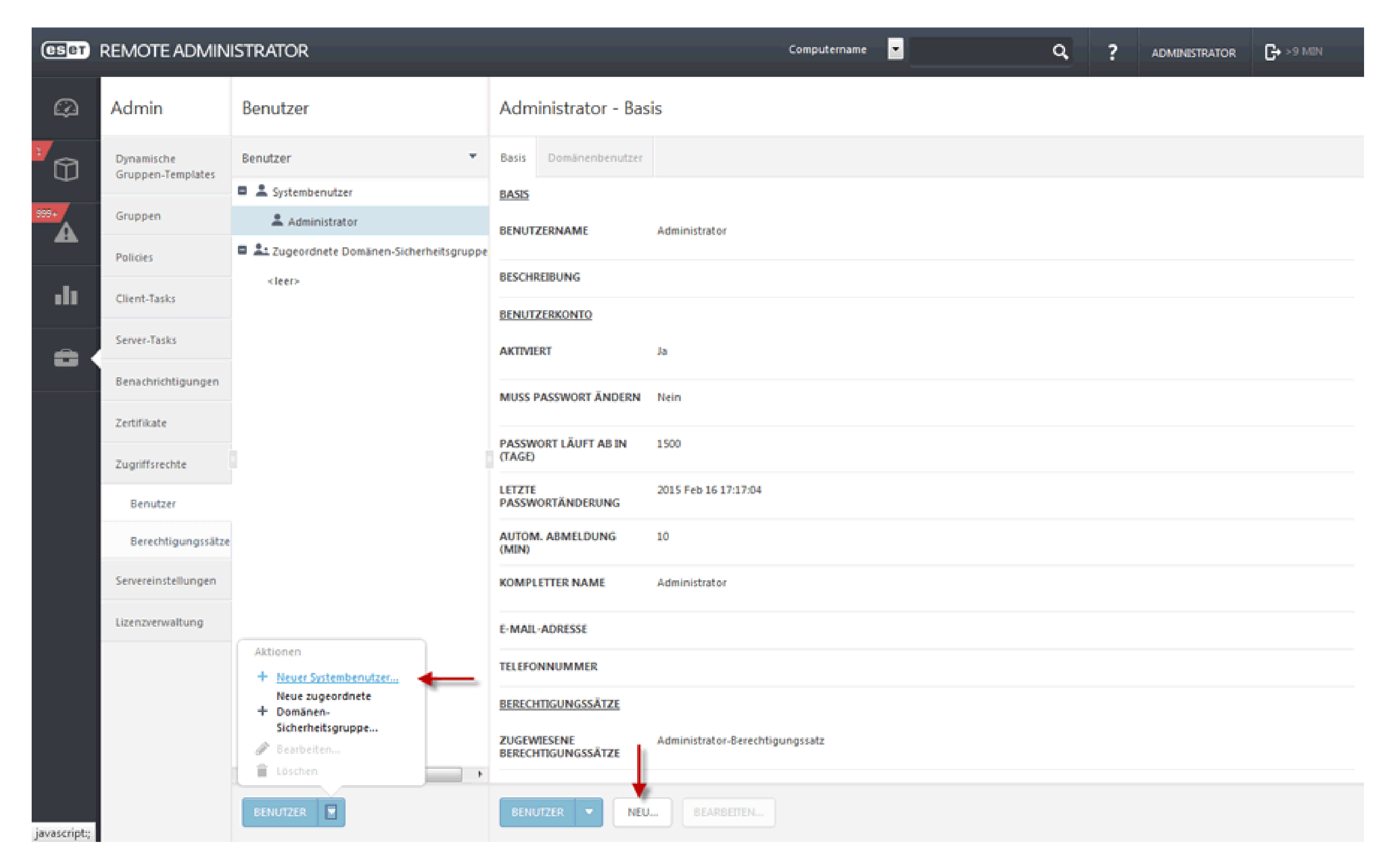
6.1.7.1.2 Assistent für Systembenutzer

Um den **Assistenten für Systembenutzer** zu öffnen, navigieren Sie zu **Admin** > **Zugriffsrechte** > **Benutzer** > **Benutzer** oder unten auf der Seite zu **Neu**.



6.1.7.1.3 Erstellen eines Systembenutzers

Um einen neuen Systembenutzer zu erstellen, klicken Sie auf der Registerkarte **Admin** auf **Zugriffsrechte** > **Benutzer** und dann unten auf der Seite auf **Benutzer** oder **Neu**.



Basis

Geben Sie einen **Benutzernamen** und optional eine **Beschreibung** für den neuen Benutzer ein.

Authentifizierung

Das Passwort des Benutzers sollte aus mindestens 8 Zeichen bestehen. Das Passwort darf nicht den Benutzernamen enthalten.

Benutzerkonto

- Lassen Sie die Option **Aktiviert** ausgewählt, es sei denn, Sie möchten (zur späteren Verwendung) ein inaktives Konto erstellen.
- Lassen Sie die Option **Muss Passwort ändern** deaktiviert. Wenn diese Option aktiviert ist, muss der Benutzer bei der ersten Anmeldung an der ERA Web-Konsole sein Passwort ändern.
- Die Option **Passwort läuft ab** legt fest, wie viele Tage das Passwort gültig ist, bevor es geändert werden muss.
- Die Option **Autom. Abmeldung (Min)** legt fest, nach wie vielen Minuten Inaktivität der Benutzer automatisch von der Web-Konsole abgemeldet wird.
- Zur Identifizierung des Benutzers können außerdem die Angaben **Kompletter Name**, **E-Mail-Adresse** und **Telefonnummer** eingegeben werden.

Berechtigungssatz

Weisen Sie dem Benutzer Berechtigungen (Rechte) zu. Sie können einen vordefinierten Berechtigungssatz auswählen: **Prüfer-Berechtigungssatz** (ähnlich Lesezugriff) und **Administrator-Berechtigungssatz** (ähnlich Vollzugriff). Alternativ können Sie einen benutzerdefinierten Berechtigungssatz erstellen.

Zusammenfassung

Überprüfen Sie die für den Benutzer konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**, um das Konto zu erstellen.

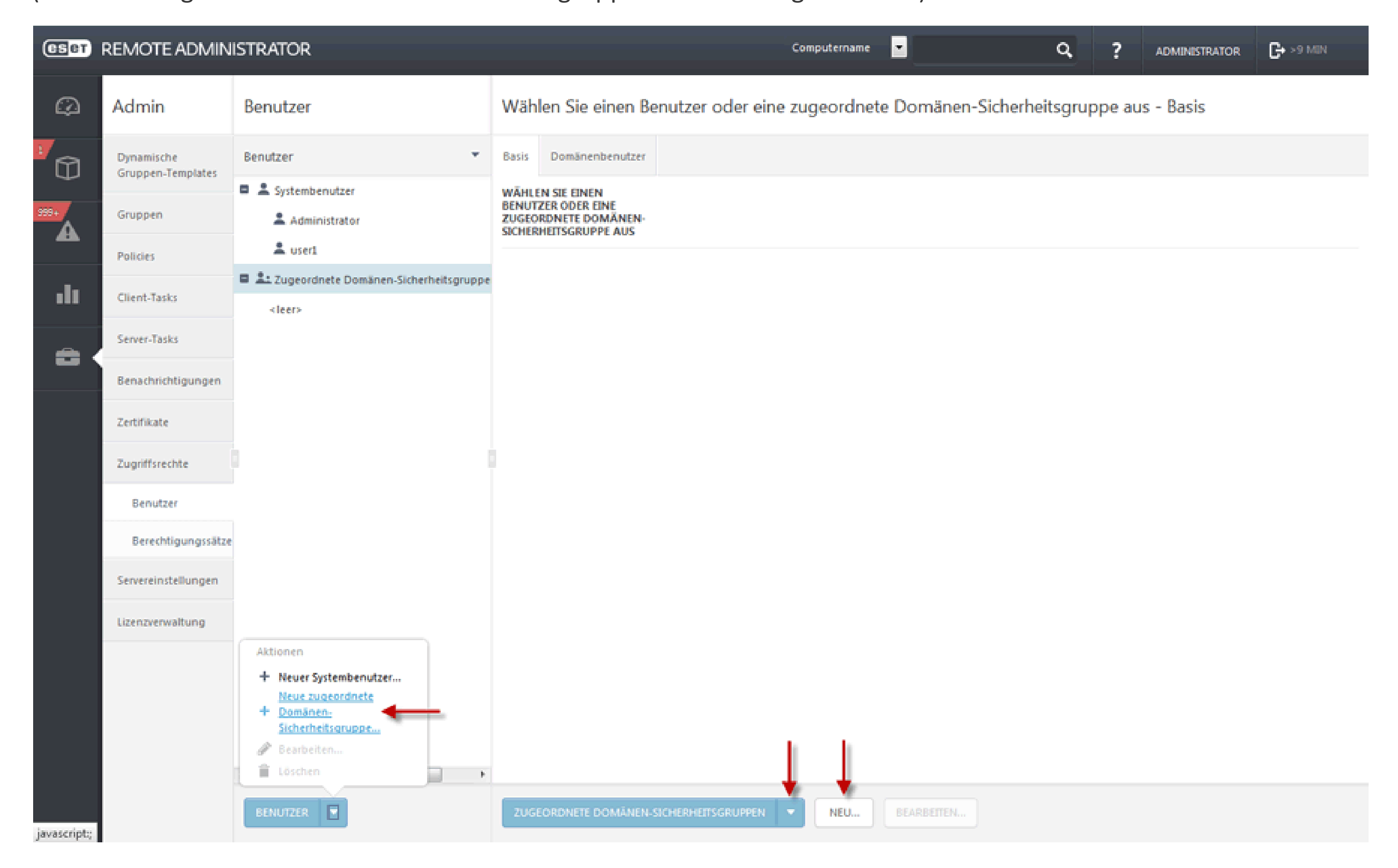
6.1.7.1.3.1 Erstellen eines neuen Administratorkontos

Um ein zweites Administratorkonto zu erstellen, befolgen Sie die Schritte unter Systembenutzer erstellen und weisen Sie dem Konto den Administratorberechtigungssatz zu.

6.1.7.1.4 Zuordnen einer Gruppe zur Domänen-Sicherheitsgruppe

Sie können dem ERA-Server eine Domänen-Sicherheitsgruppe zuordnen und zulassen, dass bestehende Benutzer (Mitglieder dieser Domänen-Sicherheitsgruppen) als Benutzer der ERA Web-Konsole übernommen werden.

Klicken Sie auf **Admin** > **Zugriffsrechte** > **Zugeordnete Domänen-Sicherheitsgruppen** > **Neu** oder einfach auf **Neu** (wenn die zugeordnete Domänen-Sicherheitsgruppe im Baum ausgewählt ist).



Basis

Domänengruppe

Geben Sie einen **Namen** für die Gruppe ein. Sie können auch eine Beschreibung der Gruppe angeben. Die Gruppe wird über eine **Gruppen-SID** (Sicherheits-ID) identifiziert. Klicken Sie auf **Auswählen**, um eine Gruppe aus der Liste auszuwählen, und dann zum Bestätigen auf **OK**.

Benutzerkonto

- Lassen Sie die Option **Aktiviert** ausgewählt, damit der Benutzer aktiv ist.
- Die Option **Autom. Abmeldung (Min)** legt fest, nach wie vielen Minuten Inaktivität der Benutzer automatisch von der Web-Konsole abgemeldet wird.
- Die Angaben **E-Mail-Adresse** und **Telefonnummer** sind fakultativ und dienen der Identifizierung des Benutzers.

Berechtigungssatz

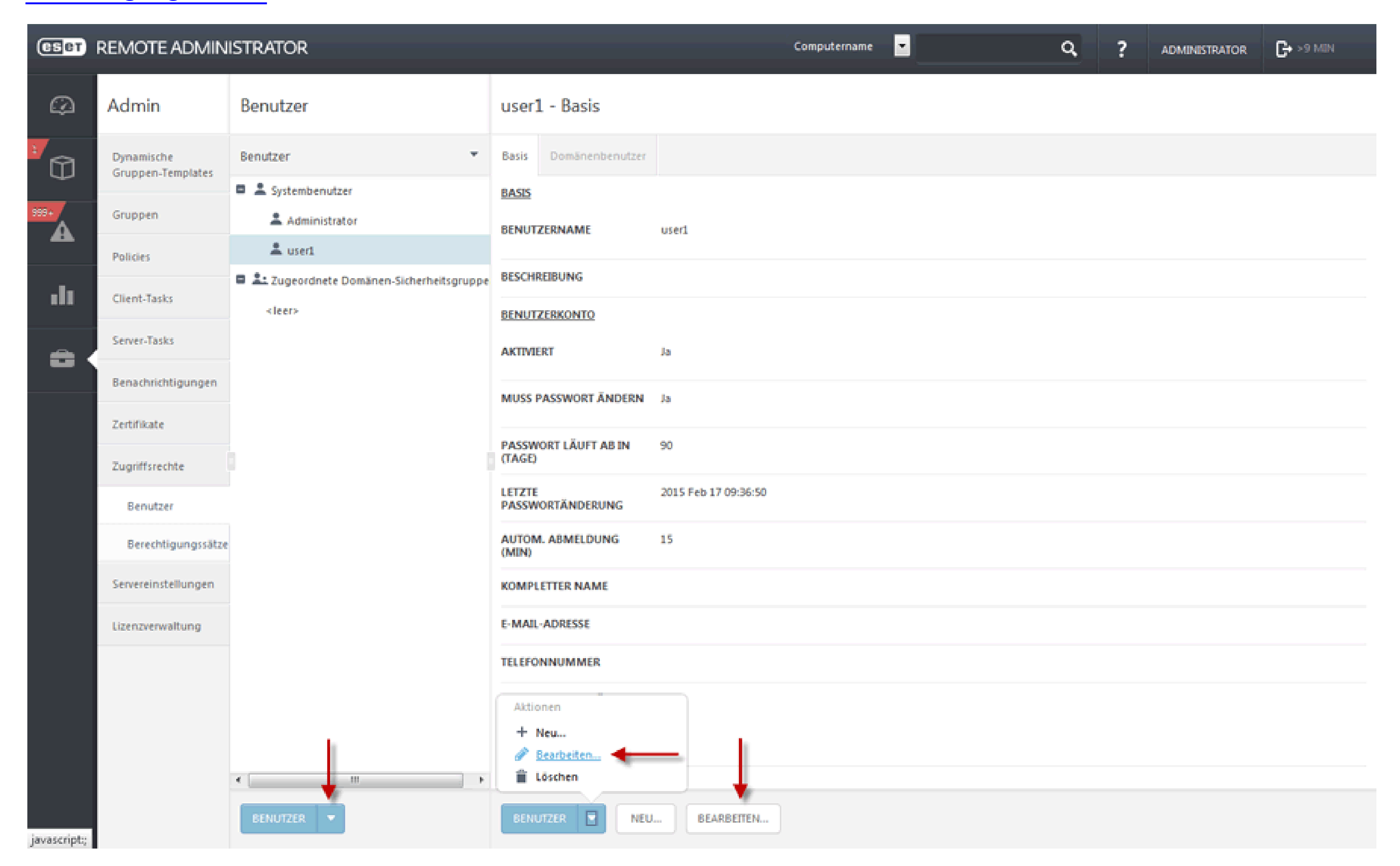
Weisen Sie dem Benutzer Berechtigungen (Rechte) zu. Sie können einen vordefinierten Berechtigungssatz verwenden: **Prüfer-Berechtigungssatz** (ähnlich Lesezugriff) und **Administrator-Berechtigungssatz** (ähnlich Vollzugriff). Alternativ können Sie einen benutzerdefinierten Berechtigungssatz erstellen.

Zusammenfassung

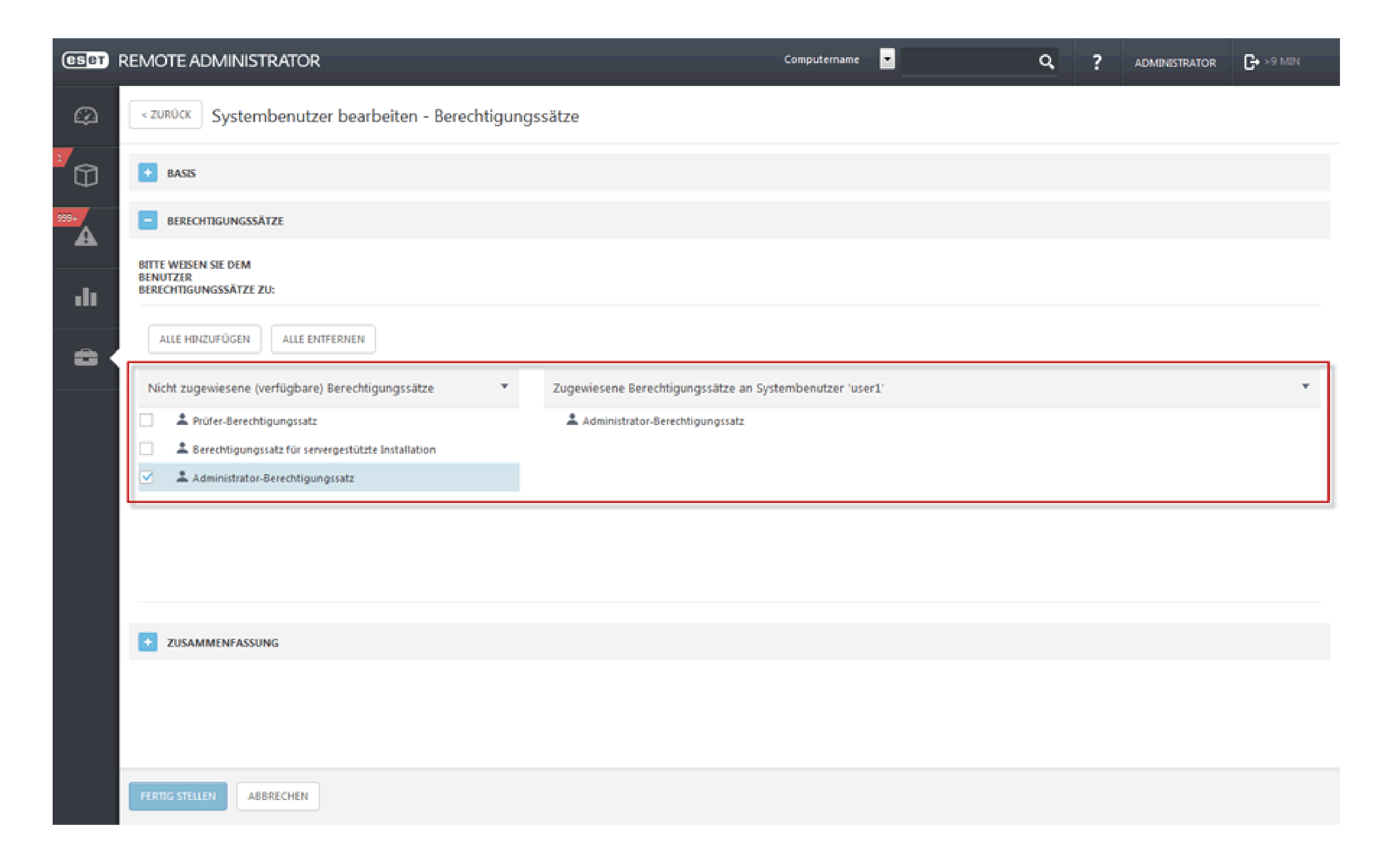
Überprüfen Sie die für den Benutzer konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**, um die Gruppe zu erstellen.

6.1.7.1.5 Zuweisen eines Berechtigungssatzes zu einem Benutzer

Wechseln Sie zu **Admin** > **Zugriffsrechte** > **Berechtigungssätze** und klicken Sie auf **Bearbeiten**, um einem Benutzer einen bestimmten Berechtigungssatz zuzuweisen. Weitere Informationen finden Sie unter Verwalten von Berechtigungssätzen.



Im Bereich **Benutzer** können Sie einen bestimmten Benutzer bearbeiten, indem Sie auf **Bearbeiten ...** klicken und im Abschnitt **Nicht zugewiesene (verfügbare) Berechtigungssätze** das Kontrollkästchen neben einem Berechtigungssatz aktivieren.



6.1.7.2 Berechtigungssätze

Ein Berechtigungssatz definiert die Berechtigungen eines Benutzers für den Zugriff auf die ERA-Web-Konsole, d. h. was der Benutzer in der Web-Konsole anzeigen bzw. welche Aktionen er ausführen kann. Systembenutzer verfügen über eigene Berechtigungen. Domänenbenutzer haben die Berechtigungen ihrer zugeordneten Sicherheitsgruppe.

Die Berechtigungen für die ERA-Web-Konsole sind in Kategorien eingeteilt, beispielsweise Systembenutzer, Zertifikate oder Policies. Für jede Funktion kann über einen Berechtigungssatz Lese- oder Schreibzugriff gewährt werden.

Nur Lesezugriff eignet sich für Benutzer, die einen Audit durchführen. Sie können Daten anzeigen, jedoch keine Änderungen vornehmen.

Benutzer mit den Rechten **Schreiben/Ausführen** können die entsprechenden Objekte ändern oder ausführen (abhängig von der Art des Objekts; Tasks beispielsweise können ausgeführt werden).

Neben den Berechtigungen für die ERA-Funktionen kann auch Zugriff auf Statische Gruppen erteilt werden. Der Zugriff wird kann für jeden Benutzer einzeln definiert werden und gilt entweder für **alle statischen Gruppen** oder für **Teilsätze der statischen Gruppen**. Der Zugriff auf eine bestimmte Statische Gruppe umfasst automatisch auch den Zugriff auf alle Untergruppen. Hierbei gilt:

- **Nur Lesezugriff** ermöglicht das Anzeigen der Computerliste.
- **Schreiben/Ausführen** gibt dem Benutzer die Berechtigung, die Computer unter Statische Gruppe zu ändern und Client-Tasks und Policies zuzuweisen.

6.1.7.2.1 Assistent für Berechtigungssätze

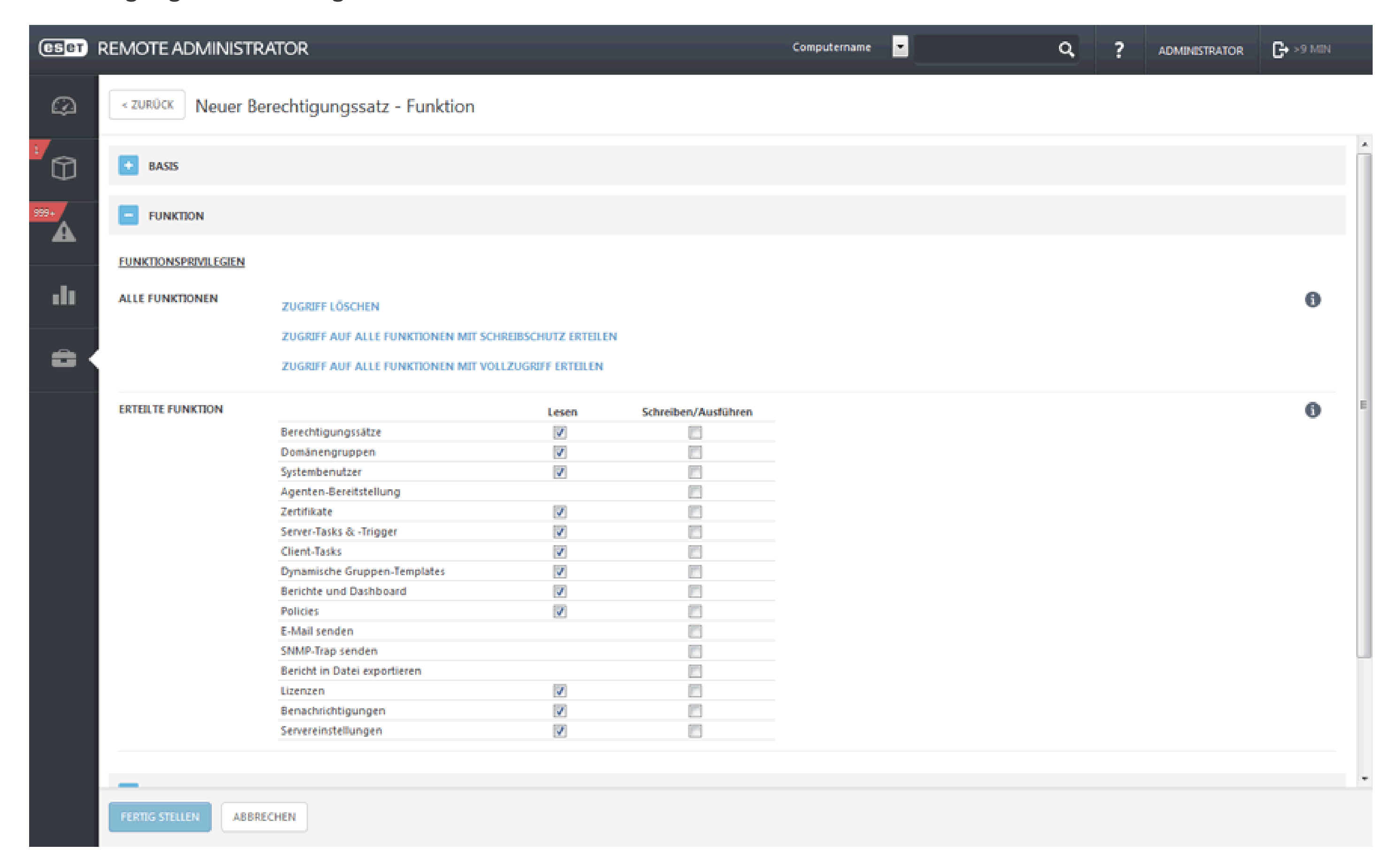
Um einen neuen Berechtigungssatz hinzuzufügen, klicken Sie auf **Berechtigungssätze** > **Neu** oder einfach auf **Neu**.

6.1.7.2.2 Verwalten von Berechtigungssätzen

Um einen bestimmten Berechtigungssatz zu ändern, klicken Sie auf den Berechtigungssatz und dann auf **Bearbeiten**. Klicken Sie auf **Kopieren**, um ein Duplikat eines Berechtigungssatzes zu erstellen, das Sie ändern und einem bestimmten Benutzer zuweisen können.

Basis

Geben Sie einen **Namen** für den Satz ein (Pflichtangabe). Sie können auch eine **Beschreibung** für den Berechtigungssatz hinzufügen.



Funktion

Wählen Sie einzelne Module aus, auf die Sie Zugriff erteilen möchten. Der Benutzer mit der zugewiesenen Berechtigung verfügt dann Zugriff auf die angegeben Tasks. Sie können auch die Option **Zugriff auf alle Funktionen mit Schreibschutz erteilen** oder **Zugriff auf alle Funktionen mit Vollzugriff erteilen** aktivieren. Diese Berechtigungen sind jedoch schon als **Administrator-Berechtigungssatz** (Vollzugriff) bzw. **Prüfer-Berechtigungssatz** (Lesezugriff) vorhanden. Durch das Erteilen der Rechte **Schreiben/Ausführen** wird automatisch auch das Recht **Lesen** erteilt.

Statische Gruppen

Sie können eine statische Gruppe (oder mehrere statische Gruppen) hinzufügen, die den Berechtigungssatz (und damit die im Abschnitt **Module** definierten Rechte) übernehmen, oder allen statischen Gruppen entweder Lesezugriff oder Vollzugriff gewähren. Sie können nur statische Gruppen hinzufügen, weil die erteilten Berechtigungssätze für bestimmte Benutzer oder Gruppen festgelegt sind.

Benutzer

Im linken Bereich werden alle verfügbaren Benutzer aufgelistet. Wählen Sie bestimmte Benutzer oder über die Schaltfläche **Alle hinzufügen** alle Benutzer aus. Die zugewiesenen Benutzer werden rechts aufgelistet.

Zusammenfassung

Überprüfen Sie die für den Berechtigungssatz konfigurierten Einstellungen und klicken Sie auf **Fertig stellen**.

6.1.8 Servereinstellungen

In diesem Bereich können Sie bestimmte Einstellungen für den ESET Remote Administrator-Server konfigurieren.

Verbindung

- **Remote Administrator-Port (Neustart erforderlich!)** – Dies ist der Port für die Verbindung zwischen dem ESET Remote Administrator-Server und den Agenten. Wenn diese Einstellung geändert wird, muss der ERA-Serverdienst neu gestartet werden, damit die Änderungen wirksam sind.
- **Port für ERA Web-Konsole (Neustart erforderlich!)** – Port für die Verbindung zwischen der Web-Konsole und dem ERA-Server.
- **Zertifikat** – Hier können Sie Zertifikate verwalten. Weitere Informationen finden Sie im Kapitel Peerzertifikate.

Updates

- **Update-Intervall** – Intervall für das Abrufen der Updates. Sie können ein regelmäßiges Intervall festlegen und die Einstellungen konfigurieren oder einen CRON-Ausdruck verwenden.
- **Update-Server** – Update-Server, von dem der ERA-Server die Updates für Sicherheitsprodukte und ERA-Komponenten empfängt.
- **Updatetyp** – Wählen Sie hier aus, welche Updatetypen Sie empfangen möchten. Zur Auswahl stehen reguläre Updates, Test-Updates und verzögerte Updates. Für ein Produktionssystem sollten Sie keine Test-Updates auswählen, da dies mit einem erhöhten Risiko verbunden ist.

Erweiterte Einstellungen

- **HTTP-Proxy** – Sie können einen Proxyserver für die Verbindung zum Internet verwenden.
- **SMTP-Server** – Sie können einen SMTP-Server zum Empfangen und Senden verschiedener Nachrichten verwenden. Hier können Sie die Einstellungen für den SMTP-Server konfigurieren.
- **Repository** – Speicherort des Repository, in dem sich die Installationsdateien befinden.
- **Logging** – Legen Sie hier die Mindestinformationen fest, die erfasst und in Logs geschrieben werden. Die Abstufung reicht von **Trace** (umfangreiche Informationen) zu **Schwerwiegend** (wichtigste, kritische Informationen).
- **Datenbank-Bereinigung** – Um eine Überlastung der Datenbank zu verhindern, können Sie mit dieser Option regelmäßig die Logs bereinigen.

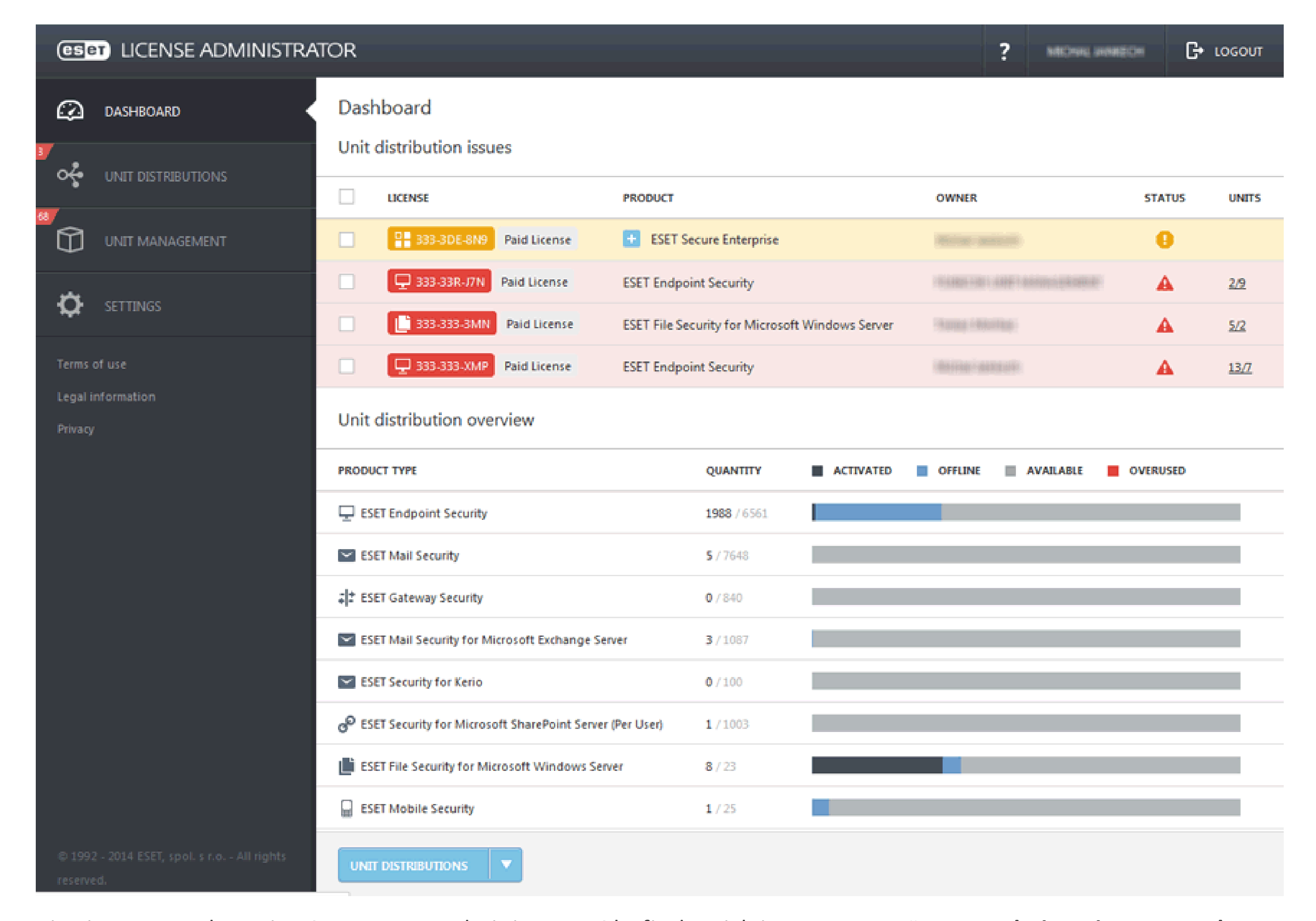
6.1.9 Lizenzverwaltung

Für ESET Remote Administrator Version 6 und höher wird ein völlig neues ESET-Lizenzsystem verwendet.

Der Benutzername und das Passwort werden durch einen **Lizenzschlüssel**/eine **Public ID** ersetzt. Der **Lizenzschlüssel** ist eine eindeutige Zeichenkette, die zur Identifizierung des Lizenzeigentümers und der Aktivierung dient. Die **Public ID** ist eine kurze Zeichenkette, mit der ein Dritter (zum Beispiel der **Sicherheitsadministrator**, der für die Einheitenverteilung verantwortlich ist) die Lizenz identifizieren kann.

Der **Sicherheitsadministrator** ist eine Person, die Lizenzen verwaltet, und muss nicht unbedingt der eigentliche **Lizenzeigentümer** sein. Der Lizenzeigentümer kann die Lizenz an einen Sicherheitsadministrator delegieren (ihn autorisieren). Wenn der Sicherheitsadministrator dies annimmt, ist er zur Verwaltung der Lizenz (Änderungen vornehmen, Einheiten zuweisen usw.) berechtigt. Der Sicherheitsadministrator kann die Lizenz zur Aktivierung von ESET-Produkten (Zuweisen einer Einheit) verwenden.

Die Lizenzen werden entweder in diesem Bereich oder online verwaltet. Für die Onlineverwaltung klicken Sie entweder auf **ELA öffnen** (ESET-Lizenzadministrator) oder öffnen Sie die Weboberfläche für den ESET-Lizenzadministrator (siehe Abschnitt Sicherheitsadministrator).



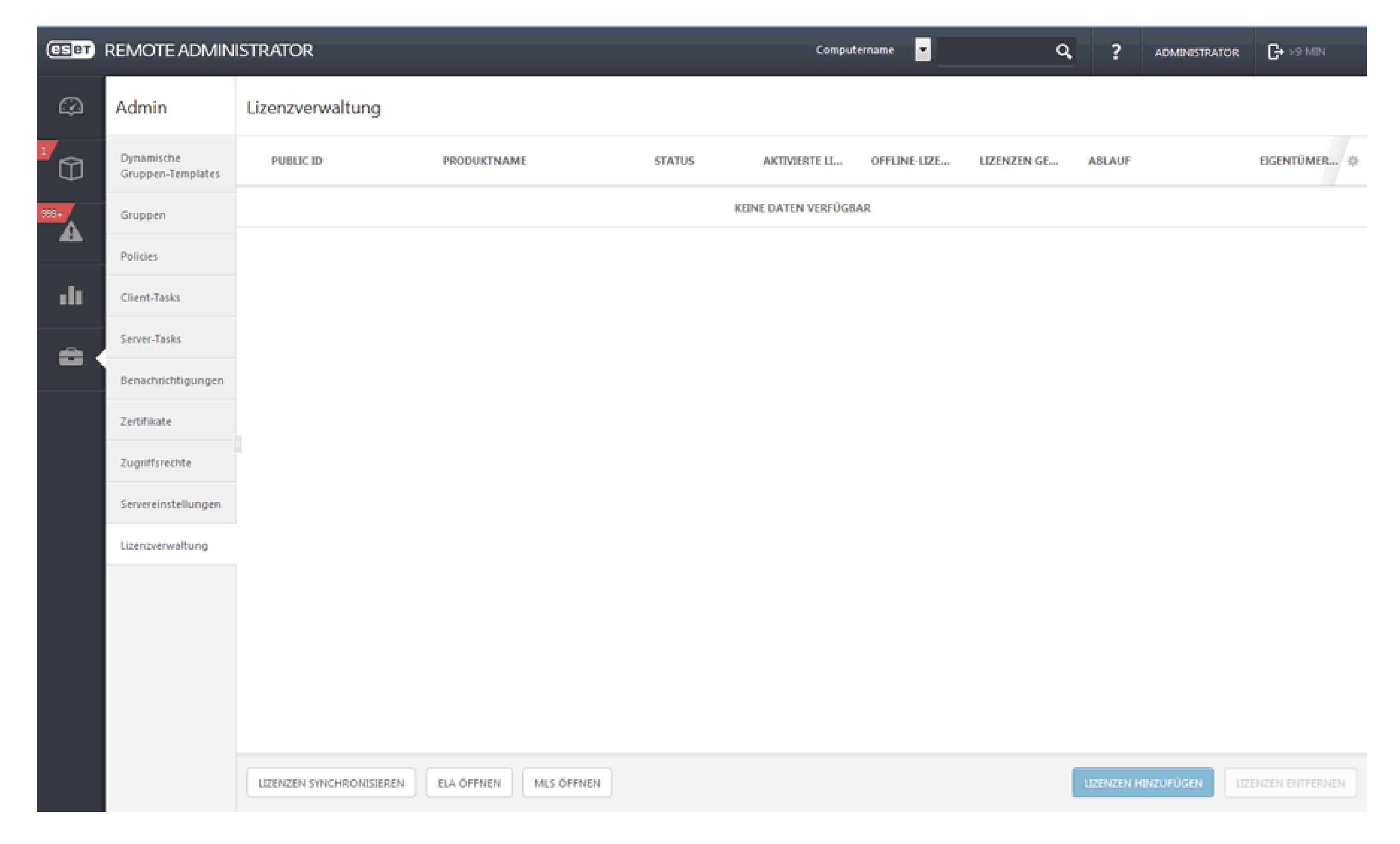
Die Lizenzverwaltung in ESET Remote Administrator 6 befindet sich im Hauptmenü unter **Admin** > **Lizenzverwaltung**.

Die Lizenzen können über zwei Tasks von ERA an die ESET-Sicherheitsprodukte verteilt werden:

- Software-Installationstask
- Produktaktivierungstask

Lizenzen werden über ihre öffentliche ID eindeutig identifiziert. Für jede Lizenz werden folgende Informationen angezeigt:

- **Produktname** des Sicherheitsprodukts, für das die Lizenz gilt
- allgemeiner **Status** der Lizenz (hier wird eine Warnmeldung angezeigt, wenn die Lizenz abgelaufen ist bzw. bald abläuft oder wenn die Lizenzgrenze überschritten wurde oder diese Gefahr besteht)
- Anzahl der **Einheiten**, die mit der Lizenz aktiviert werden können
- Ablaufdatum der Lizenz
- **Eigentümer** der Lizenz und **Kontakt**.



Lizenzen synchronisieren

Die Lizenz-Synchronisierung mit ESET License Administrator erfolgt automatisch täglich. Wenn Sie Änderungen in ESET License Administrator vornehmen und die aktuellen Lizenzinformationen sofort in ERA erscheinen sollen anstatt nach der nächsten Synchronisierung, klicken Sie auf die Schaltfläche **Lizenzen synchronisieren**.

Lizenz oder Lizenzschlüssel hinzufügen

Klicken Sie auf „Lizenzen hinzufügen“ und wählen Sie die gewünschte Methode zum Hinzufügen der neuen Lizenz(en) aus:

1. Lizenzschlüssel: Geben Sie den Lizenzschlüssel einer gültigen Lizenz ein und klicken sie auf **Lizenz hinzufügen**. Der Lizenzschlüssel wird auf dem Aktivierungsserver überprüft und zur Liste hinzugefügt.

2. Anmeldedaten des Sicherheitsadministrators: Verknüpfen Sie ein Sicherheitsadministratorkonto und alle verbundenen Lizenzen mit dem Bereich **Lizenzverwaltung**.

3. Lizenzdatei - Fügen Sie eine Lizenzdatei (.lic) hinzu und klicken Sie auf **Lizenz hinzufügen**. Die Lizenzdatei wird überprüft und die Lizenz zur Liste hinzugefügt.

Lizenzen entfernen

Wählen Sie eine Lizenz aus der Liste oben aus und klicken Sie auf diese Option, um sie vollständig zu entfernen. Sie werden aufgefordert, diese Aktion zu bestätigen. Beim Entfernen der Lizenzen wird das Produkt nicht deaktiviert. Das ESET-Produkt bleibt aktiv, selbst wenn die Lizenz in der ERA-Lizenzverwaltung gelöscht wurde.

6.1.9.1 Aktivierung

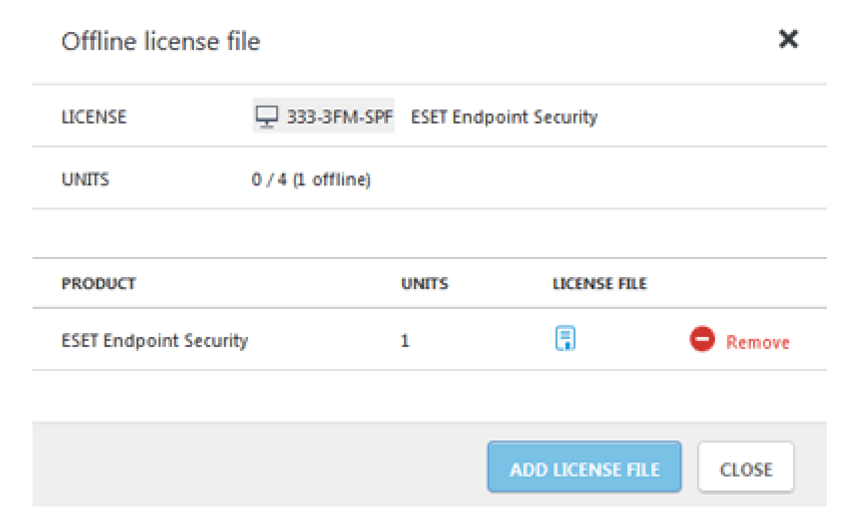
Öffnen Sie **Admin** > **Lizenzverwaltung** und klicken Sie auf **Lizenzen hinzufügen**.

- Geben Sie in das entsprechende Feld den **Lizenzschlüssel** ein, den Sie beim Kauf der ESET-Sicherheitslösung erhalten haben. Sie können den Lizenzschlüssel kopieren und einfügen, oder eintippen. Wenn Sie über einen alten Lizenznachweis (in Form von Benutzername und Passwort) verfügen, konvertieren Sie die Anmeldedaten in einen Lizenzschlüssel. Wenn die Lizenz nicht registriert ist, wird der Registrierungsvorgang ausgelöst. Dieser erfolgt im ELA-Portal (ERA stellt je nach Ursprung der Lizenz eine für die Registrierung gültige URL bereit).

- Geben Sie die Anmeldedaten für den **Sicherheitsadministrator** ein (die delegierten Lizenzen werden später im ERA-Lizenzmanager angezeigt).

- Geben Sie die **Offline-Lizenzdatei** ein. Diese muss über das ELA-Portal exportiert werden. Fügen Sie die Informationen über die von ERA zu verwaltenden Produkte hinzu. Zum Generieren der Offline-Lizenzdatei müssen Sie im ESET-Lizenzadministrator-Portal ein spezifisches **Lizenzdatei-Token** eingeben. Andernfalls wird die Lizenzdatei von ESET Remote Administrator nicht akzeptiert.

Klicken Sie auf das Dokumentsymbol, um die Offline-Lizenzdatei zu speichern.



Wechseln Sie wieder zur ERA-Lizenzverwaltung, klicken Sie auf „Lizenzen hinzufügen“, suchen Sie nach der in ELA exportierten Offline-Lizenzdatei und klicken Sie dann auf **Hochladen**.

7. Diagnose-Tool

Das Diagnose-Tool ist in allen ERA-Komponenten enthalten. Es dient dem Erfassen und Erstellen von Logs, die Entwicklern zur Behebung von Problemen mit den Produktkomponenten dienen. Führen Sie das Diagnose-Tool aus, wählen Sie einen Stammordner zum Speichern der Logs und legen Sie die Aktionen fest (siehe **Aktionen** weiter unten).

Das **Diagnose-Tool** finden Sie hier:

Windows

Ordner *C:\Program Files\ESET\RemoteAdministrator\<product>*, Datei **Diagnostic.exe**.

Linux

Pfad auf dem Server: */opt/eset/RemoteAdministrator/<product>/*. Hier finden Sie die ausführbare Datei **Diagnostic<Produkt>** (in einem Wort, beispielsweise **DiagnosticServer**, **DiagnosticAgent**).

Aktionen

- **Dump-Logs** – Ein Log-Ordner zum Speichern der Logs wird erstellt.
- **Dump-Prozess** – Es wird ein neuer Ordner erstellt. Eine Prozess-Dumpdatei wird üblicherweise erstellt, wenn ein Problem erkannt wurde. Im Falle eines schwerwiegenden Problems erstellt das System eine Dumpdatei. Sie können dies manuell überprüfen, indem Sie im Ordner %temp% (Windows) bzw. /tmp/ (Linux) eine DMP-Datei einfügen.
  HINWEIS: Der Dienst (Agent, Proxy, Server, RD Sensor, FileServer) muss ausgeführt werden.
- **Allgemeine Anwendungsinformationen** – Der Ordner GeneralApplicationInformation und die darin enthaltene Datei GeneralApplicationInformation.txt werden erstellt. Diese Datei enthält Textinformationen wie den Produktnamen und die Produktversion des aktuell installierten Produkts.
- **Aktionskonfiguration** – Ein Konfigurationsordner wird erstellt, in dem die Datei storage.lua gespeichert wird.

8. Glossar

8.1 Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die versucht, in einen Computer einzudringen und/oder auf einem Computer Schaden anzurichten.

8.1.1 Viren

Bei einem Computervirus handelt es sich um eingedrungene Schadsoftware, die Dateien auf Ihrem Computer beschädigt. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich von einem zum anderen Computer auszubreiten.

Computerviren greifen hauptsächlich ausführbare Dateien und Dokumente an. Um sich zu vermehren, hängt sich ein Virus mit seinem „Körper“ an das Ende einer Zieldatei. Und so funktioniert ein Computervirus: Durch Ausführung der infizierten Datei wird der Virus aktiviert (noch bevor die eigentliche Anwendung gestartet wird) und führt seinen vordefinierten Task aus. Erst dann wird die eigentliche Anwendung gestartet. Ein Virus kann einen Computer also nur dann infizieren, wenn der Benutzer selbst (versehentlich oder absichtlich) das bösartige Programm ausführt oder öffnet.

Computerviren unterscheiden sich nach Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen Schaden verursachen. Ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Viren werden (im Vergleich zu Trojanern oder Spyware) immer seltener, da sie keinen kommerziellen Nutzen für ihre Urheber haben. Außerdem wird der Begriff „Virus“ oft fälschlicherweise für alle Arten von Schadsoftware verwendet. Heute setzt sich mehr und mehr der neue, treffendere Ausdruck „Malware“ (engl. bösartige Software) durch.

Wenn Ihr Computer mit einem Virus infiziert wurde, ist es notwendig, den Originalzustand der infizierten Dateien wiederherzustellen, das heißt, den Schadcode mithilfe eines Virenschutzprogrammes daraus zu entfernen.

Beispiele für Viren sind: OneHalf, Tenga und Yankee Doodle.

8.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das bösartigen Code enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Sie sind unabhängig von Hostdateien (oder Bootsektoren). Würmer verbreiten sich über die E-Mail-Adressen in Ihrer Kontaktliste oder nutzen Sicherheitslücken von Anwendungen in Netzwerken.

Daher sind Würmer wesentlich funktionsfähiger als Computerviren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden und sogar Minuten über den gesamten Globus verbreiten. Da sich Würmer unabhängig und rasant vermehren können, sind sie gefährlicher als andere Arten von Schadsoftware.

Ein innerhalb eines Systems aktivierter Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Schadcode fungieren.

Wurde Ihr Computer mit einem Wurm infiziert, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcode enthalten.

Zu den bekanntesten Würmern zählen: Lovsan/Blaster, Stration/Warezov, Bagle und Netsky.

8.1.3 Trojaner

Trojaner galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten. Dies gilt jedoch nur für die Trojaner von damals. Heutzutage müssen sich Trojaner nicht mehr tarnen. Ihr einzige Absicht besteht darin, sich möglichst leicht Zugang zu einem System zu verschaffen, um dort den gewünschten Schaden anzurichten. Der Ausdruck „Trojaner“ ist zu einem sehr allgemeinen Begriff geworden, der jegliche Form von Schadsoftware beschreibt, die nicht einer bestimmten Kategorie zugeordnet werden kann.

Aus diesem Grund wird die Kategorie „Trojaner“ oft in mehrere Gruppen unterteilt.

- **Downloader** - Ein bösartiges Programm zum Herunterladen von Schadsoftware aus dem Internet.
- **Dropper** - Trojaner, der auf angegriffenen Computern weitere Schadsoftware absetzt („droppt“).
- **Backdoor** - Anwendung, die Angreifern Zugriff auf ein System verschafft, um es zu kontrollieren.
- **Keylogger** - Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet.
- **Dialer** - Dialer sind Programme, die Verbindungen zu teuren Einwahlnummern herstellen. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Diese werden allerdings nur noch selten eingesetzt.

Trojaner sind in der Regel ausführbare Dateien mit der Erweiterung EXE. Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Zu den bekanntesten Trojanern zählen: NetBus, Trojandownloader. Small.ZL, Slapper

8.1.4 Rootkits

Rootkits sind bösartige Programme, die Hackern unbegrenzten und verdeckten Zugriff auf ein System verschaffen. Nach dem Zugriff auf ein System (in der Regel unter Ausnutzung einer Sicherheitslücke) greifen Rootkits auf Funktionen des Betriebssystems zurück, um nicht von der Virenschutz-Software erkannt zu werden: Sie verdecken Prozesse, Dateien, Windows-Registrierungsdaten usw. Aus diesem Grund können sie mit herkömmlichen Prüfmethoden kaum erfasst werden.

Rootkits können auf zwei verschiedenen Ebenen entdeckt werden:

1) Beim Zugriff auf ein System. Die Rootkits haben das System noch nicht befallen, sind also inaktiv. Die meisten Virenschutzsysteme können Rootkits auf dieser Ebene entfernen (vorausgesetzt, dass solche Dateien auch als infizierte Dateien erkannt werden).
2) Wenn die Rootkits sich vor den regulären Prüfmethoden verstecken. Benutzer von ESET Remote Administrator profitieren von der Anti-Stealth-Technologie, die auch aktive Rootkits erkennen und entfernen kann.

8.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, die zur Anzeige von Werbung dienen. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, damit deren Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich - allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist Adware, insofern sie auch dazu dienen kann, Daten zu sammeln (wie es bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren.

In einigen Fällen lassen sich Programme jedoch nicht ohne die Adware installieren, oder nur mit eingeschränktem Funktionsumfang. Das bedeutet, dass Adware häufig ganz „legal“ auf das System zugreift, da sich der Benutzer damit einverstanden erklärt hat. In diesem Fall gilt: Vorsicht ist besser als Nachsicht. Wird auf Ihrem Computer ein Adware-Programm entdeckt, sollten Sie die Datei löschen, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

8.1.6 Spyware

Der Begriff „Spyware“ fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/ Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. eine Liste der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Entwickler von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten enthalten möglicherweise Sicherheitscodes, PINs, Kontonummern usw. Spyware wird oft im Paket mit der kostenlosen Version eines Programms angeboten, um so Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die zusammen mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutzprogramme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

8.1.7 Potenziell unsichere Anwendungen

Es gibt zahlreiche seriöse Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie aber in die falschen Hände geraten, kann mit ihnen Schaden angerichtet werden. Mit ESET Remote Administrator können solche Bedrohungen erkannt werden.

Zur Kategorie der „potenziell unsicheren Anwendungen“ zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu zählen beispielsweise Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Keylogger (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen Sie die Anwendung.

8.1.8 Eventuell unerwünschte Anwendungen

Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Die gravierendsten Veränderungen sind:

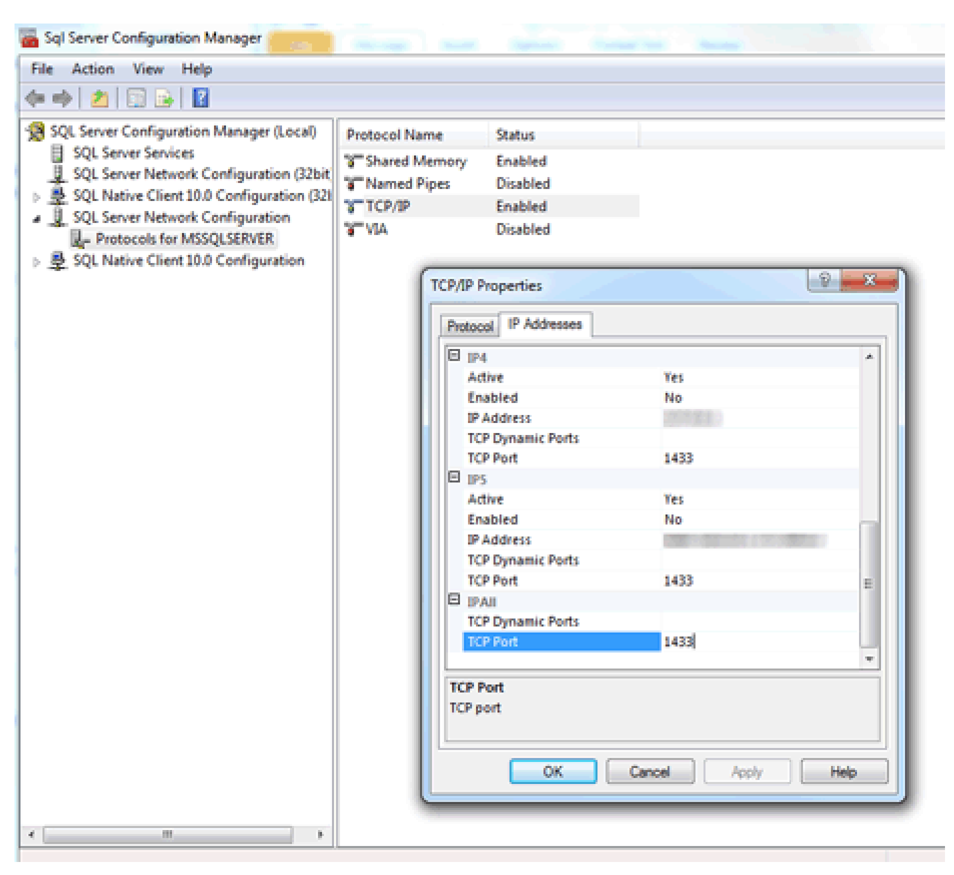
- Neue Fenster werden angezeigt
- Versteckte Prozesse werden ausgeführt
- Prozessor und Speicher werden stärker belastet als zuvor
- Suchergebnisse ändern sich
- Die Anwendung kommuniziert mit Servern im Internet

9. Häufig gestellte Fragen (FAQ)

F: Warum wird Java auf einem Server installiert? Stellt das nicht ein Sicherheitsrisiko dar?
A: Die ERA Web-Konsole benötigt Java. Java ist ein Branchenstandard für webbasierte Konsolen. Obwohl die ERA Web-Konsole mindestens Java Version 7 benötigt, empfehlen wir dringend die Verwendung der aktuellsten offiziellen Java-Version.

F: Die folgende Fehlermeldung taucht immer wieder in der trace.log-Datei von ESET Rogue Detector auf: *2015-02-25 18:55:04 Information: CPCAPDeviceSniffer [Thread 764]: CPCAPDeviceSniffer on rpcap://\Device\NPF_{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error: Fehler beim Öffnen des Geräts:Fehler beim Öffnen des Adapters: Das System hat das angegebene Gerät nicht gefunden. (20)*
A: Dabei handelt es sich um ein WinPcap-Problem. Halten Sie den ESET Rogue Detector Sensor-Dienst an, installieren Sie die neueste WinPcap-Version (mindestens 4.1.0), und starten Sie den ESET Rogue Detector Sensor--Dienst neu.

F: Wie finde ich auf einfache Weise die Portnummer meines SQL-Servers heraus?
A: Sie haben mehrere Möglichkeiten, die SQL-Portnummer zu ermitteln. Der Konfigurationsmanager des SQL-Servers bietet die genauesten Ergebnisse. Das nachstehende Beispiel zeigt, wo Sie diese Informationen im SQL-Konfigurationsmanager finden:



F: Nach der Installation von SQL Express 2008 (im ERA-Paket enthalten) auf Windows Server 2012 scheint SQL Express 2008 nicht auf einem standardmäßigen SQL-Port zu überwachen.
A: Sicherlich erfolgt die Überwachung auf einem anderen Port als dem standardmäßigen Port 1433.

F: Wie konfiguriere ich MySQL so, dass es große Pakete akzeptiert?
A: Suchen Sie die MySQL-Konfigurationsdatei (**my.ini** unter Windows bzw. **my.cnf** unter Linux; der genaue Speicherort der INI-Datei variiert je nach Betriebssystem), öffnen Sie die Datei und suchen Sie den Abschnitt `[mysqld]`. Fügen Sie die neue Zeile `max_allowed_packet=33M` hinzu (der Wert muss mindestens 33 M sein).

F: Wenn ich SQL selbst installiere: Wie erstelle ich eine Datenbank für ERA?
A: Das ist nicht erforderlich. Die Datenbank wird vom Installationsprogramm **Server.msi** erstellt, nicht vom ERA-Installationsprogramm. Das ERA-Installationsprogramm soll bestimmte Schritte für Sie vereinfachen und installiert SQL-Server. Die Datenbank wird vom Installationsprogramm „Server.msi" erstellt.

F: Kann das ERA-Installationsprogramm eine neue Datenbank in einer vorhandenen SQL Server-Installation erstellen, wenn ich die richtigen Verbindungsinformationen und Anmeldedaten für SQL Server angebe? Es wäre gut, wenn das Installationsprogramm verschiedene Versionen von SQL Server (2008, 2014 usw.) unterstützen würde!
A: Die Datenbank wird von **Server.msi**erstellt. Es kann eine ERA-Datenbank in separat installierten SQL Server-Instanzen erstellt werden. Die unterstützten Versionen von SQL Server sind 2008, 2012 und 2014.

F: Warum wird im ERA-Installationsprogramm die SQL-Version 2008 R2 verwendet?
A: Die SQL-Version 2008 R2 wird verwendet, weil Microsoft für diesen Datenbanktyp die Kompatibilität mit Windows XP und späteren Versionen des Betriebssystems bestätigt.

F: Wie sollte ich vorgehen, wenn der folgende **Fehlercode angezeigt wird: -2068052081** angezeigt wird?
A: Starten Sie Ihren Computer neu und führen Sie die Einrichtung erneut aus. Wenn dies nicht funktioniert, deinstallieren Sie SQL Server Native Client und führen Sie die Installation erneut aus. Wenn das Problem weiterhin auftritt, deinstallieren Sie alle Microsoft SQL Server-Produkte, führen Sie einen Neustart aus und wiederholen Sie die Installation.

F: Wie sollte ich vorgehen, wenn der folgende **Fehlercode angezeigt wird: -2067922943** angezeigt wird?
A: Vergewissern Sie sich, dass Ihr System die Datenbankanforderungen für ERA erfüllt.

F: Sollte bei der Installation in einem vorhandenen SQL Server standardmäßig der integrierte Windows-Authentifizierungsmodus verwendet werden?
A: Nein. Der Windows-Authentifizierungsmodus kann auf SQL Server deaktiviert werden. Die einzige Möglichkeit der Anmeldung ist die SQL Server-Authentifizierung (Eingabe von Benutzername und Passwort). Sie müssen entweder die SQL Server-Authentifizierung oder den gemischten Modus verwenden. Wenn Sie SQL Server manuell installieren, empfehlen wir, ein Root-Passwort für SQL Server zu erstellen (der Root-Benutzer ist „sa" für „Sicherheitsadministrator") und zur späteren Verwendung an einem sicheren Ort aufzubewahren. Das Root-Passwort wird evtl. zur Aufrüstung des ERA-Servers benötigt.

F: Ich musste **Microsoft .NET Framework 3.5** installieren, weil das ERA-Installationsprogramm mich dazu aufgefordert hat (http://www.microsoft.com/en-us/download/details.aspx?id=21). Dies hat jedoch in einer Erstinstallation von Windows Server 2012 R2 mit SP1 nicht funktioniert.
A: Das Installationsprogramm kann aufgrund der Sicherheitsrichtlinie von Windows Server 2012 nicht unter Windows Server 2012 verwendet werden. Verwenden Sie zur Installation von Microsoft .NET Framework den **Assistenten zum Hinzufügen von Rollen und Features**.

F: Microsoft .NET 4.5 Framework war bereits auf meinem System installiert. Ich musste .NET 3.5 mit dem Assistenten zum Hinzufügen von Rollen und Features hinzufügen. Warum funktioniert dies nicht unter 4.5?
A: .NET 4.5 ist nicht mit .NET 3.5 abwärtskompatibel, einer Voraussetzung für das SQL Server-Installationsprogramm.

F: Es ist nicht erkennbar, ob die SQL Server-Installation tatsächlich ausgeführt wird. Liegt ein Problem vor, wenn die Installation länger als 10 Minuten dauert?
A: Die SQL Server-Installation kann in seltenen Fällen bis zu 1 Stunde dauern. Die Installationsdauer hängt von der Systemleistung ab.

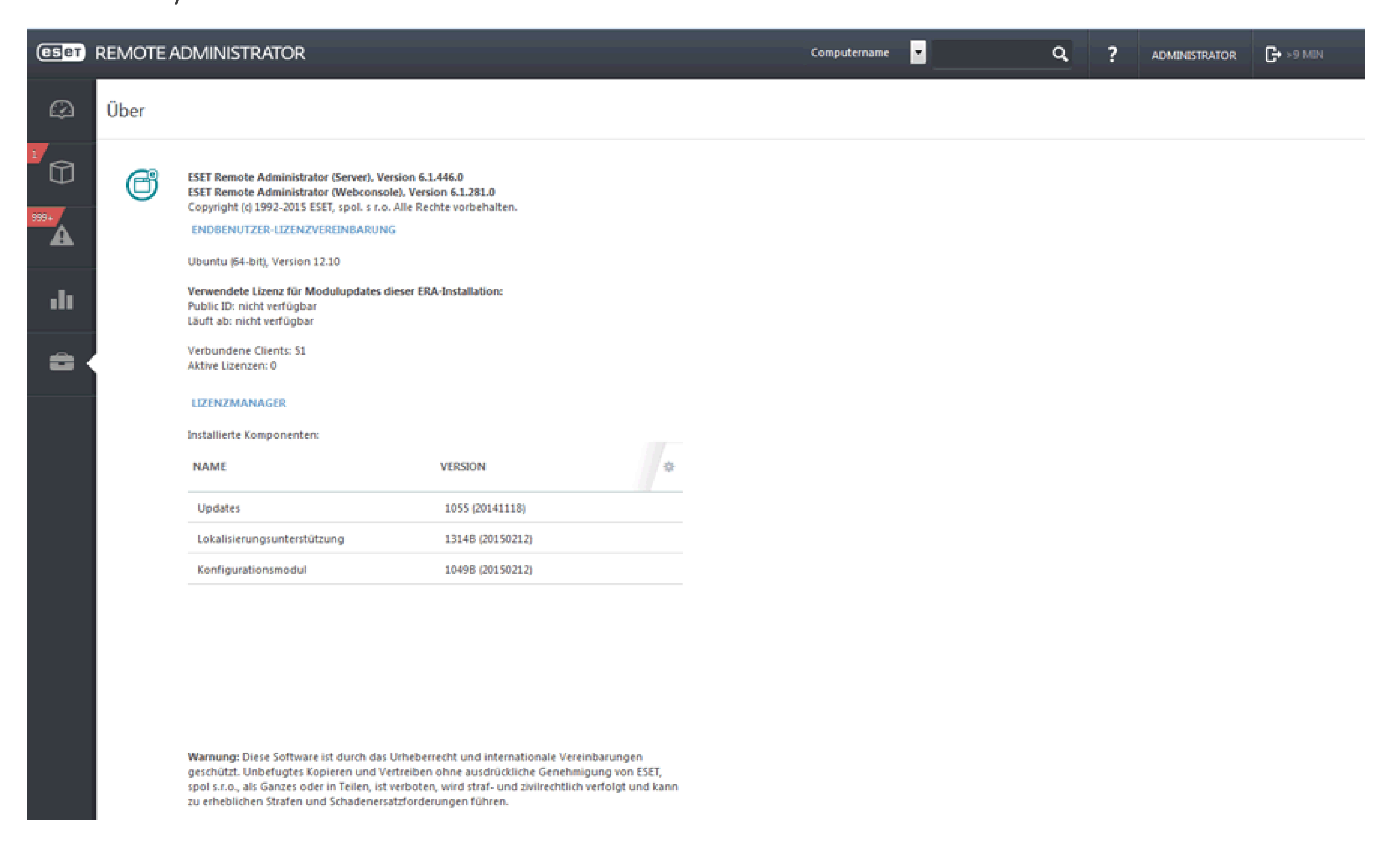
F: Wie kann ich das während der Einrichtung für die Web-Konsole eingegebene **Administratorpasswort zurücksetzen**?
A: Sie können das Passwort zurücksetzen, indem Sie das Serverinstallationsprogramm ausführen und die Option **Reparieren** auswählen. Sie brauchen jedoch evtl. das Passwort für die ERA-Datenbank, falls Sie bei der Erstellung der Datenbank keine Windows-Authentifizierung verwendet haben.

HINWEIS: Verwenden Sie diese Funktion mit Bedacht, da manche Reparaturoptionen gespeicherte Daten entfernen können.

F: Welches Dateiformat wird für den Import einer Liste von Computern benötigt, die zu ERA hinzugefügt werden sollen?
A: Datei mit den folgenden Zeilen:
All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX
Alle ist der erforderliche Name der Stammgruppe.

10. Über ESET Remote Administrator

In diesem Fenster werden Informationen zur installierten Version von ESET Remote Administrator und die Liste der installierten Programmmodule angezeigt. Der obere Teil des Fensters enthält Informationen zum Betriebssystem und zu den Systemressourcen.



11. Endbenutzer-Lizenzvereinbarung (EULA)

WICHTIGER HINWEIS: Vor dem Herunterladen, Installieren, Kopieren oder Verwenden des Produkts lesen Sie bitte die folgenden Nutzungsbedingungen. **DURCH DAS HERUNTERLADEN, INSTALLIEREN, KOPIEREN ODER VERWENDEN DER SOFTWARE ERKLÄREN SIE SICH MIT DEN NUTZUNGSBEDINGUNGEN EINVERSTANDEN**.

Endbenutzer-Softwarelizenzvereinbarung.

Diese Endbenutzer-Softwarelizenzvereinbarung (die „Vereinbarung“) zwischen ESET, spol. s r. o., mit Sitz in Einsteinova 24, 851 01 Bratislava, Slowakische Republik, Handelsregistereintrag 3586/B in der Rubrik Sro beim Amtsgericht Bratislava I, Firmennummer 31 333 535, oder einer anderen Gesellschaft aus der ESET-Unternehmensgruppe (im Folgenden „ESET“ oder „Anbieter“) und Ihnen, einer natürlichen oder juristischen Person („Sie“ oder der „Endbenutzer“), berechtigt Sie zur Nutzung der in Abschnitt 1 dieser Vereinbarung definierten Software. Die in Abschnitt 1 dieser Vereinbarung definierte Software darf unter den im Folgenden aufgeführten Bedingungen auf einem Datenträger gespeichert, per E-Mail versendet, aus dem Internet oder von Servern des Anbieters heruntergeladen oder auf andere Weise beschafft werden.

DIESES DOKUMENT IST KEIN KAUFVERTRAG, SONDERN EINE VEREINBARUNG ÜBER DIE RECHTE DES ENDBENUTZERS. Der Anbieter bleibt Eigentümer des Exemplars der Software und, soweit vorhanden, des physischen Mediums, auf dem die Software für den Verkauf vorliegt, sowie aller Kopien der Software, zu deren Erstellung der Endbenutzer unter den Bedingungen dieser Vereinbarung berechtigt ist.

Durch Klicken auf die Schaltfläche „Ich stimme zu“ beim Installieren, Herunterladen, Kopieren oder Verwenden der Software erklären Sie sich mit den Bestimmungen und Bedingungen dieser Vereinbarung einverstanden. Wenn Sie mit einer der Bestimmungen dieser Vereinbarung nicht einverstanden sind, klicken Sie auf die Schaltfläche „Ablehnen“ oder „Ich stimme nicht zu“. Brechen Sie den Download oder die Installation der Software ab, vernichten oder geben Sie die Software, das Installationsmedium, die zugehörige Dokumentation und den Erwerbsnachweis an ESET oder an dem Ort, an dem Sie die Software erhalten haben, zurück.

MIT DER NUTZUNG DER SOFTWARE ZEIGEN SIE AN, DASS SIE DIESE VEREINBARUNG GELESEN UND VERSTANDEN HABEN UND DASS SIE DIESER VEREINBARUNG ZUGESTIMMT HABEN.

1. **Software**. Mit „Software“ wird in dieser Vereinbarung bezeichnet: (i) das Computerprogramm ESET Remote Administrator , einschließlich aller seiner Teile; (ii) der Inhalt von Festplatten, CD-ROMs, DVDs, E-Mails mit Anhängen, soweit vorhanden, oder anderer Medien, denen diese Vereinbarung beiliegt, einschließlich Software, die in Form von Objektcode auf einem Datenträger, per E-Mail oder als Internet-Download zur Verfügung gestellt wird; (iii) sämtliche Anleitungs- und Dokumentationsmaterialien zur Software, insbesondere jegliche Art von Beschreibungen der Software, ihre Spezifikation, Beschreibungen von Eigenschaften und Programmbetrieb, Beschreibungen der Umgebung, in der die Software verwendet wird, Betriebs- oder Installationshandbüchern oder jegliche Beschreibungen zur richtigen Verwendung der Software („Dokumentation“); (iv) Kopien der Software, Fehlerbehebungsmaßnahmen für die Software, soweit vorhanden, Ergänzungen und Erweiterungen der Software, veränderte Versionen der Software und, falls vorhanden, sämtliche Aktualisierungen von Teilen der Software, für die Ihnen der Anbieter die Lizenz gemäß Abschnitt 3 dieser Vereinbarung gewährt. Der Anbieter stellt die Software ausschließlich in Form von ausführbarem Objektcode zur Verfügung.

2. **Installation**. Die Software, sei sie auf einem Datenträger bereitgestellt, per E-Mail versendet, aus dem Internet oder von den Servern des Anbieters heruntergeladen oder aus anderen Quellen bezogen, erfordert eine Installation. Die Software muss auf einem korrekt konfigurierten Computer installiert werden, der den in der Dokumentation angegebenen Mindestanforderungen entspricht. Die Vorgehensweise zur Installation ist in der Dokumentation angegeben. Auf dem Computer, auf dem Sie die Software installieren, dürfen keine Computerprogramme oder Hardware vorhanden sein, durch die die Software beeinträchtigt werden könnte.

3. **Lizenz**. Unter der Voraussetzung, dass Sie sich mit dieser Vereinbarung einverstanden erklärt haben, sämtliche darin enthaltenen Bestimmungen einhalten und die jeweilige Lizenzgebühr zum Fälligkeitstermin entrichten, gewährt Ihnen der Anbieter die folgenden Rechte (die „Lizenz“):

a) **Installation und Nutzung**. Sie erhalten das nicht exklusive und nicht übertragbare Recht, die Software auf der Festplatte eines Computers oder einem ähnlichen Medium zur dauerhaften Datenspeicherung zu installieren, die Software im Arbeitsspeicher eines Computers zu speichern und die Software auf Computern zu implementieren, zu speichern und anzuzeigen.

b) **Anzahl der Lizenzen**. Das Nutzungsrecht für die Software ist durch die Anzahl der Endbenutzer beschränkt. Unter einem „Endbenutzer“ ist Folgendes zu verstehen: (i) die Installation der Software auf einem Computer; wenn der Umfang einer Lizenz sich nach der Anzahl von Postfächern richtet, ist ein Endbenutzer (ii) ein Computerbenutzer, der E-Mail über ein E-Mail-Programm empfängt. Wenn das E-Mail-Programm E-Mail empfängt und diese anschließend automatisch an mehrere Benutzer weiterleitet, richtet sich die Anzahl der Endbenutzer nach der tatsächlichen Anzahl von Benutzern, an die auf diesem Weg E-Mail-Nachrichten gesendet werden. Wenn ein Mailserver die Funktion eines E-Mail-Gateways ausführt, entspricht die Zahl der Endbenutzer der Anzahl von Mailservern, für die dieses Gateway Dienste bereitstellt. Wenn mehrere E-Mail-Adressen (beispielsweise durch Aliasnamen) von einem Benutzer verwendet werden und nur ein Benutzer über diese Adressen E-Mail empfängt, während auf Clientseite keine E-Mail-Nachrichten automatisch an mehrere Benutzer verteilt werden, ist nur eine Lizenz für einen Computer erforderlich. Die gleichzeitige Nutzung derselben Lizenz auf mehreren Computern ist untersagt.

c) **Business Edition**. Für die Verwendung der Software auf E-Mail-Servern, E-Mail-Relays, E-Mail- oder Internet-Gateways ist die Business Edition der Software erforderlich.

d) **Laufzeit der Lizenz**. Ihr Nutzungsrecht für die Software ist zeitlich beschränkt.

e) **OEM-Software**. OEM-Software darf ausschließlich auf dem Computer genutzt werden, mit dem Sie sie erhalten haben. Eine Übertragung auf einen anderen Computer ist nicht gestattet.

f) **Nicht für den Wiederverkauf bestimmte Software und Testversionen**. Nicht für den Wiederverkauf („not for resale“, NFR) oder als Testversion bereitgestellte Software darf nicht veräußert, sondern ausschließlich zum Vorführen oder Testen der Softwarefunktionen verwendet werden.

g) **Ablauf und Kündigung der Lizenz**. Die Lizenz läuft automatisch zum Ende des jeweiligen Lizenzzeitraums aus. Sollten Sie eine Ihrer Pflichten aus dieser Vereinbarung verletzen, ist der Anbieter berechtigt, diese außerordentlich zu kündigen und, ggf. auf dem Rechtsweg, etwaige weitere Ansprüche geltend zu machen. Bei Ablauf oder Kündigung der Lizenz müssen Sie die Software und ggf. alle Sicherungskopien sofort löschen, zerstören oder auf eigene Kosten an ESET oder das Geschäft zurückgeben, in dem Sie die Software erworben haben.

4. **Internetverbindung**. Für den korrekten Betrieb der Software ist eine Internetverbindung erforderlich, da die Software in regelmäßigen Abständen Verbindungen zu den Servern des Anbieters bzw. anderen externen Servern aufbauen muss. Ohne eine Internetverbindung können die folgenden Funktionen der Software nicht genutzt werden:

a) **Software-Updates**. Der Anbieter hat das Recht, von Zeit zu Zeit Aktualisierungen für die Software („Updates“) bereitzustellen, ist hierzu jedoch nicht verpflichtet. Diese Funktion ist in den Standardeinstellungen der Software aktiviert. Die Updates werden also automatisch installiert, sofern der Endbenutzer dies nicht deaktiviert hat.

b) **Weiterleitung von eingedrungener Schadsoftware und anderen Informationen an den Anbieter**. Die Software enthält eine Funktion zur Erfassung neuer Computerviren oder anderer, ähnlich schädlicher Computerprogramme sowie von verdächtigen oder problematischen Dateien (im Folgenden „eingedrungene Schadsoftware“). Diese Daten werden, zusammen mit Informationen über den Computer und/oder die Plattform, auf der die Software installiert ist (im Folgenden „Informationen“), an den Anbieter gesendet. Die Informationen können Daten (auch persönliche Daten) über den Endbenutzer und/oder andere Benutzer des Computers enthalten, auf dem die Software installiert ist. Sie können außerdem Informationen über den Computer, das Betriebssystem, über installierte Programme sowie über Dateien des Computers, auf dem die Software installiert ist, und von Schadsoftware betroffenen Dateien mit sämtlichen Informationen über diese Dateien umfassen. Der Anbieter verwendet die erhaltenen Informationen und die ihm übermittelte eingedrungene Schadsoftware ausschließlich zur Untersuchung des eingedrungenen Codes. Er trifft angemessene Maßnahmen, damit die erhaltenen Informationen vertraulich behandelt werden. Durch Ihre Zustimmung zu dieser Vereinbarung und Aktivierung der oben genannten Softwarefunktion erklären Sie sich damit einverstanden, dass eingedrungene Schadsoftware und Informationen an den Anbieter weitergeleitet werden. Gleichzeitig erklären Sie gemäß den geltenden rechtlichen Bestimmungen Ihre Zustimmung zur Verarbeitung der erhaltenen Informationen.

5. **Ausübung der Rechte des Endbenutzers**. Sie müssen Ihre Rechte als Endbenutzer selbst oder gegebenenfalls über Ihre Angestellten ausüben. Als Endbenutzer dürfen Sie die Software ausschließlich zur Gewährleistung der Arbeitsfähigkeit und zum Schutz derjenigen Computer verwenden, für die Sie eine Lizenz erworben haben.

6. **Beschränkungen der Rechte**. Es ist untersagt, die Software zu kopieren, zu verbreiten oder aufzuteilen. Außerdem dürfen keine abgeleiteten Versionen erstellt werden. Für die Nutzung der Software gelten die folgenden Einschränkungen:

(a) Sie dürfen eine Kopie der Software auf einem Medium zur dauerhaften Speicherung als Sicherungskopie erstellen, vorausgesetzt die Sicherungskopien werden nicht auf einem anderen Computer installiert oder verwendet. Das Erstellen jeder weiteren Kopie der Software verstößt gegen diese Vereinbarung.

(b) Jegliche von den Bestimmungen dieser Vereinbarung abweichende Nutzung, Modifikation, Übersetzung oder Reproduktion der Software sowie die Einräumung von Rechten zur Nutzung der Software oder von Kopien der Software ist untersagt.

(c) Die Software darf nicht an andere Personen verkauft, sublizenziert oder vermietet werden. Ebenso darf die Software nicht von einer anderen Person gemietet, einer anderen Person ausgeliehen oder zur gewerbsmäßigen Erbringung von Dienstleistungen verwendet werden.

(d) Der Quellcode der Software darf nicht durch Reverse-Engineering analysiert, dekompiliert oder disassembliert oder auf andere Weise beschafft werden, soweit eine solche Beschränkung nicht ausdrücklich gesetzlichen Bestimmungen widerspricht.

(e) Sie verpflichten sich, die Software nur in Übereinstimmung mit allen am Verwendungsort geltenden gesetzlichen Bestimmungen zu verwenden, insbesondere gemäß den Beschränkungen, die sich aus dem Urheberrecht und anderen Rechten an geistigem Eigentum ergeben.

7. **Urheberrecht**. Die Software und alle Rechte einschließlich des Rechtstitels und der geistigen Eigentumsrechte daran sind Eigentum von ESET und/oder seiner Lizenzgeber. Sie unterliegen dem Schutz der Bestimmungen internationaler Abkommen und aller sonstigen geltenden Gesetze des Landes, in dem die Software verwendet wird. Die Struktur, die Aufteilung und der Code der Software sind Geschäftsgeheimnisse und vertrauliche Informationen von ESET und/oder seiner Lizenzgeber. Die Software darf nicht kopiert werden, wobei lediglich die in Abschnitt 6(a) angegebene Ausnahme gilt. Alle gemäß dieser Vereinbarung zulässigen Kopien müssen dieselben Urheberrechts- und Eigentümerhinweise wie die ursprüngliche Software enthalten. Wenn Sie in Verstoß gegen die Bestimmungen dieser Vereinbarung Quellcode durch Reverse-Engineering analysieren, dekompilieren oder disassemblieren oder versuchen, sich den Quellcode auf andere Weise zu beschaffen, gehen automatisch sämtliche dadurch gewonnenen Informationen unwiderruflich und unmittelbar in das Eigentum des Anbieters über. Weiterhin ist der Anbieter in diesem Fall berechtigt, etwaige weitere Ansprüche aus Ihrem Verstoß gegen diese Vereinbarung geltend zu machen.

8. **Rechtevorbehalt**. Mit Ausnahme der Rechte, die Ihnen als Endbenutzer der Software in dieser Vereinbarung ausdrücklich gewährt werden, behält sich der Anbieter alle Rechte an der Software vor.

9. **Versionen in verschiedenen Sprachen/auf mehreren Datenträgern, mehrere Exemplare**. Wenn die Software mehrere Plattformen oder Sprachen unterstützt, oder wenn Sie mehrere Exemplare der Software erhalten haben, darf die Software nur auf derjenigen Anzahl von Computern und nur in den Versionen verwendet werden, für die Sie eine Lizenz erworben haben. Es dürfen keine Versionen oder Kopien der Software, die von Ihnen nicht verwendet werden, an andere Personen verkauft, vermietet, sublizenziert, verliehen oder auf diese übertragen werden.

10. **Beginn und Gültigkeitsdauer der Vereinbarung**. Diese Vereinbarung tritt an dem Tag in Kraft, an dem Sie sich mit ihren Bestimmungen einverstanden erklären. Sie können diese Vereinbarung jederzeit kündigen, indem Sie die Software, alle Sicherungskopien und, falls vorhanden, alle vom Anbieter oder seinen Geschäftspartnern zur Verfügung gestellten zugehörigen Materialien dauerhaft löschen, sie zerstören bzw. auf eigene Kosten zurückgeben. Unabhängig von der Gültigkeitsdauer dieser Vereinbarung und der Art und Weise ihres Ablaufs bzw. ihrer Kündigung behalten die Bestimmungen der Abschnitte 7, 8, 11, 13, 20 und 22 auf unbegrenzte Zeit ihre Gültigkeit.

11. **AUSDRÜCKLICHE ERKLÄRUNGEN DES ENDBENUTZERS**. ALS ENDBENUTZER ERKENNEN SIE AN, DASS DIE SOFTWARE IM JEWEILIGEN IST-ZUSTAND UND OHNE JEGLICHE AUSDRÜCKLICHE ODER KONKLUDENTE GEWÄHRLEISTUNG BEREITGESTELLT WIRD, SOWEIT DIES IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG IST. WEDER DER ANBIETER NOCH SEINE LIZENZGEBER ODER DIE RECHTEINHABER GEWÄHREN AUSDRÜCKLICHE ODER KONKLUDENTE ZUSICHERUNGEN ODER GEWÄHRLEISTUNGEN, INSBESONDERE KEINE ZUSICHERUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON PATENTEN, URHEBER- UND MARKENRECHTEN ODER SONSTIGEN RECHTEN DRITTER. ES BESTEHT VON SEITEN DES ANBIETERS ODER DRITTER KEINERLEI GEWÄHRLEISTUNG, DASS DIE IN DER SOFTWARE ENTHALTENEN FUNKTIONEN IHREN ANFORDERUNGEN ENTSPRECHEN ODER DASS DIE SOFTWARE STÖRUNGS- UND FEHLERFREI AUSGEFÜHRT WIRD. SIE ÜBERNEHMEN DIE VOLLE VERANTWORTUNG UND DAS VOLLE RISIKO HINSICHTLICH DER AUSWAHL DER SOFTWARE ZUM ERREICHEN DER VON IHNEN BEABSICHTIGTEN ERGEBNISSE SOWIE FÜR INSTALLATION UND NUTZUNG DER SOFTWARE UND DEN MIT DIESER ERZIELTEN ERGEBNISSEN.

12. **Keine weiteren Verpflichtungen**. Aus dieser Vereinbarung ergeben sich für den Anbieter und seine Lizenzgeber keine weiteren Verpflichtungen außer den explizit aufgeführten.

13. **HAFTUNGSAUSSCHLUSS**. SOWEIT IM RAHMEN DER GELTENDEN GESETZE ZULÄSSIG, ÜBERNEHMEN DER ANBIETER, SEINE ANGESTELLTEN UND SEINE LIZENZGEBER KEINERLEI HAFTUNG FÜR ENTGANGENE GEWINNE, ERTRÄGE ODER VERKÄUFE. VON DER HAFTUNG AUSGESCHLOSSEN SIND AUSSERDEM DATENVERLUSTE, BESCHAFFUNGSKOSTEN FÜR ERSATZTEILE ODER DIENSTE, SACH- UND PERSONENSCHÄDEN, GESCHÄFTSUNTERBRECHUNGEN, DER VERLUST VON GESCHÄFTSINFORMATIONEN SOWIE JEGLICHE ANDERE NEBEN-, VERMÖGENS- ODER FOLGESCHÄDEN, DIE INFOLGE DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE ENTSTEHEN. DIES GILT UNABHÄNGIG VON DER RECHTSGRUNDLAGE DES VORGEBRACHTEN ANSPRUCHS (VERTRAGSHAFTUNG, DELIKTISCHE HAFTUNG, FAHRLÄSSIGKEIT USW.) UND AUCH DANN, WENN DER ANBIETER, SEINE LIZENZGEBER ODER VERBUNDENE UNTERNEHMEN ÜBER DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS IN KENNTNIS GESETZT WURDEN. DA IN BESTIMMTEN LÄNDERN UND UNTER BESTIMMTEN GESETZEN EIN HAFTUNGSAUSSCHLUSS NICHT ZULÄSSIG IST, EINE HAFTUNGSBESCHRÄNKUNG JEDOCH MÖGLICH, BESCHRÄNKT SICH DIE HAFTUNG DES ANBIETERS, SEINER ANGESTELLTEN UND LIZENZGEBER AUF DEN FÜR DIE LIZENZ ENTRICHTETEN PREIS.

14. Gesetzlich verankerte Verbraucherrechte haben im Konfliktfall Vorrang vor den Bestimmungen dieser Vereinbarung.

15. **Technischer Support**. ESET bzw. die von ESET beauftragten Dritten erbringen jeglichen technischen Support ausschließlich nach eigenem Ermessen und ohne diesbezügliche Zusicherungen oder Gewährleistungen. Der Endbenutzer ist verpflichtet, vor der Inanspruchnahme von Supportleistungen eine Sicherungskopie aller vorhandenen Daten, Softwareanwendungen und sonstigen Programme zu erstellen. ESET bzw. die von ESET beauftragten Dritten übernehmen keinerlei Haftung für Datenverluste, Sach- und Vermögensschäden (insb. Schäden an Software und Hardware) oder entgangene Gewinne infolge der Erbringung von Supportleistungen. ESET bzw. die von ESET beauftragten Dritten sichern nicht zu, dass ein bestimmtes Problem auf dem Wege des technischen Support gelöst werden kann, und behalten sich das Recht vor, die Arbeit an einem Problem ggf. einzustellen. ESET behält sich das Recht vor, die Erbringung von Supportleistungen nach eigenem Ermessen vorübergehend auszusetzen, ganz einzustellen oder im konkreten Einzelfall abzulehnen.

16. **Übertragung der Lizenz**. Die Software darf von einem Computersystem auf ein anderes übertragen werden, sofern dabei nicht gegen Bestimmungen dieser Vereinbarung verstoßen wird. Sofern in dieser Vereinbarung nicht anderweitig geregelt, ist es dem Endbenutzer gestattet, die Lizenz und alle Rechte aus dieser Vereinbarung an einen anderen Endbenutzer zu übertragen, sofern der Anbieter dem zustimmt und die folgenden Voraussetzungen beachtet werden: (i) Der ursprüngliche Endbenutzer darf keine Kopien der Software zurückbehalten. (ii) Die Übertragung der Rechte muss direkt erfolgen, d. h. vom ursprünglichen Endbenutzer an den neuen Endbenutzer. (iii) Der neue Endbenutzer muss sämtliche Rechte und Pflichten des ursprünglichen Endbenutzers aus dieser Vereinbarung übernehmen. (iv) Der ursprüngliche Endbenutzer muss dem neuen Endbenutzer einen der in Abschnitt 17 genannten Nachweise für die Gültigkeit des Softwarelizenz übereignen.

17. **Gültigkeitsnachweis für die Softwarelizenz**.Der Endbenutzer kann seine Nutzungsrechte an der Software auf eine der folgenden Arten nachweisen: (i) über ein Lizenzzertifikat, das vom Anbieter oder einem von diesem beauftragten Dritten ausgestellt wurde; (ii) über eine schriftliche Lizenzvereinbarung, falls abgeschlossen; (iii) durch Vorlage einer E-Mail des Anbieters mit den Lizenzdaten (Benutzername und Passwort) für Updates.

18. **Daten über den Endbenutzer und Datenschutzbestimmungen**. Als Endbenutzer erlauben Sie dem Anbieter das Übertragen, Verarbeiten und Speichern der Daten, anhand derer der Anbieter Sie identifizieren kann. Sie erklären sich einverstanden, dass der Anbieter mit eigenen Mitteln überprüfen kann, ob Sie die Software in Übereinstimmung mit den Bedingungen dieser Vereinbarung verwenden. Sie erklären sich einverstanden, dass zwischen der Software und den Computersystemen des Anbieters oder seiner Geschäftspartner Daten übertragen werden können. Dies dient zur Sicherstellung der Funktionalität und Berechtigung zur Nutzung der Software und dem Schutz der Rechte des Anbieters. Mit Abschluss dieser Vereinbarung willigen Sie zudem in die Übertragung, Verarbeitung und Speicherung Ihrer personenbezogenen Daten durch den Anbieter bzw. seine Geschäftspartner ein, soweit eine solche Nutzung zur Abrechnung und zur Erfüllung dieser Vereinbarung erforderlich ist. Details zur Privatsphäre und zum Schutz personenbezogener Daten finden Sie unter http://www.eset.com/privacy.

19. **Lizenzvergabe an Behörden und die US-Regierung**. Für die Lizenzvergabe an Behörden, insbesondere an Stellen der US-Regierung, gelten ausschließlich die in dieser Vereinbarung beschriebenen Lizenzrechte und Einschränkungen.

20. **Export- und Reexportbestimmungen**. Die Software, die Dokumentation bzw. Teile derselben, einschließlich der Informationen über die Software und Teile derselben, unterliegen Überwachungsmaßnahmen für Importe und Exporte. Diese richten sich nach rechtlichen Bestimmungen, die von den jeweiligen Regierungen nach geltendem Gesetz verabschiedet werden können. Insbesondere betrifft dies US-Gesetze, Exportbestimmungen sowie Einschränkungen zu bestimmten Endbenutzern, Nutzungsarten und Zielländern, die von der US-Regierung bzw. anderen Regierungen erlassen werden. Sie verpflichten sich, alle geltenden Import- und Exportbestimmungen einzuhalten, und bestätigen, dass Sie selbst verantwortlich für die Beschaffung ggf. erforderlicher Genehmigungen für den Export, Reexport, Transfer oder Import der Software sind.

21. **Kündigungen**. Alle Kündigungen sowie zurückgegebene Software und Dokumentation sind an folgende Adresse zu senden: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slowakische Republik.

22. **Geltendes Recht, Gerichtsstand**. Diese Vereinbarung unterliegt slowakischem Recht. Der Endbenutzer und der Anbieter vereinbaren, dass gesetzliche Bestimmungen zur Konfliktlösung und UN-Kaufrecht nicht zur Anwendung kommen. Sie erklären sich ausdrücklich damit einverstanden, dass als Gerichtsstand für alle Streitfälle mit dem Anbieter oder bezüglich Ihrer Verwendung der Software das Amtsgericht Bratislava I, Slowakische Republik vereinbart wird.

23. **Allgemeine Bestimmungen**. Wenn eine der Bestimmungen dieser Vereinbarung ungültig oder uneinklagbar sein sollte, beeinträchtigt dies nicht die Gültigkeit der übrigen Bestimmungen der Vereinbarung. Diese bleiben unter den hier festgelegten Bedingungen gültig und einklagbar. Änderungen an dieser Vereinbarung bedürfen der Schriftform und müssen von einem bevollmächtigten Vertreter des Anbieters unterzeichnet werden.

Bei dieser Vereinbarung zwischen Ihnen und dem Anbieter handelt es sich um die einzige für diese Software geltende Vereinbarung. Sie ersetzt alle vorhergehenden, die Software betreffenden Zusicherungen, Mitteilungen, Übereinkünfte oder Werbeinformationen.